ALIBABA CLOUD

Alibaba Cloud

云服务器ECS

安全

文档版本：20220708

阿里云

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. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	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。
注意	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。
说明	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	命令或代码。	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.安全最佳实践

本文介绍在创建和使用实例过程中提高实例安全性的做法。

背景信息

安全涵盖的范围广泛，阿里云保证自身云基础设施和服务的安全，例如机房、虚拟化平台等，但您在使用云产品过程中遵循安全实践同样重要，例如流量控制、机密信息保管、权限控制等。

使用账号安全功能

阿里云提供账号相关的安全功能，帮助您在账号级别防范风险。

- 为阿里云账号启用多因素认证MFA。

  启用MFA后，登录阿里云控制台时需要输入账号密码和MFA设备实时生成的动态验证码，在账号密码泄露时也可以阻止未授权访问，提高账号安全性。

- 使用RAM用户和用户组在账号级别对资源进行访问控制。

  在多用户需要协同操作资源的场景中，建议避免直接共享使用阿里云账号。共享阿里云账号的密钥等机密信息会大大增加泄露风险，一旦泄露会威胁账号下所有资源的安全。建议使用访问控制RAM创建RAM用户和用户组，并授予各RAM用户和用户组最小权限，可以有效降低风险。

  RAM用户对应企业内的员工、系统或应用程序，您可以按需为RAM用户授予最小的访问权限。如果分工明确，您还可以通过用户组分类职责相同的RAM用户，提高批量管理效率。示例如下：

  i. 为需要创建和管理资源的职位创建SysAdmins用户组，并添加权限策略，授予执行所有操作的权限。
  ii. 为需要使用资源的职位创建Developers用户组，并添加权限策略，授予调用StartInstance、StopInstance、DescribeInstances接口的权限。
  iii. 为员工创建RAM用户，并按照各自职位加入用户组。
  iv. 为加强网络安全控制，添加权限策略，规定如果组内用户的IP地址不是来自企业网络，则拒绝其访问资源。
  v. 如果某开发人员的职位变更为系统管理员，将其RAM用户从Developers用户组移动到SysAdmins用户组 。
  vi. 如果Developers用户组的RAM用户需要更大权限，修改用户组的权限策略即可应用到用户组中的所有RAM用户。

  更多信息，请参见通过RAM用户控制资源访问。

- 使用实例RAM角色避免泄露AccessKey。

  如果实例上部署的应用程序需要访问阿里云其他云产品（例如OSS、VPC、RDS等）的API，请避免将AccessKey固化在实例中，例如写在配置文件中，这种方式有很高的泄露风险。

  建议使用实例RAM角色，为实例绑定实例RAM角色后，可以基于STS（Security Token Service）临时凭证访问其他云产品的API，即可以保证云账号AccessKey安全，还可以借助访问控制RAM实现精细化控制和权限管理。更多信息，请参见实例RAM角色概述。

创建实例时启用安全合规特性

阿里云提供了实例规格、云盘加密等满足实例安全合规要求的特性，您可以按需选择。

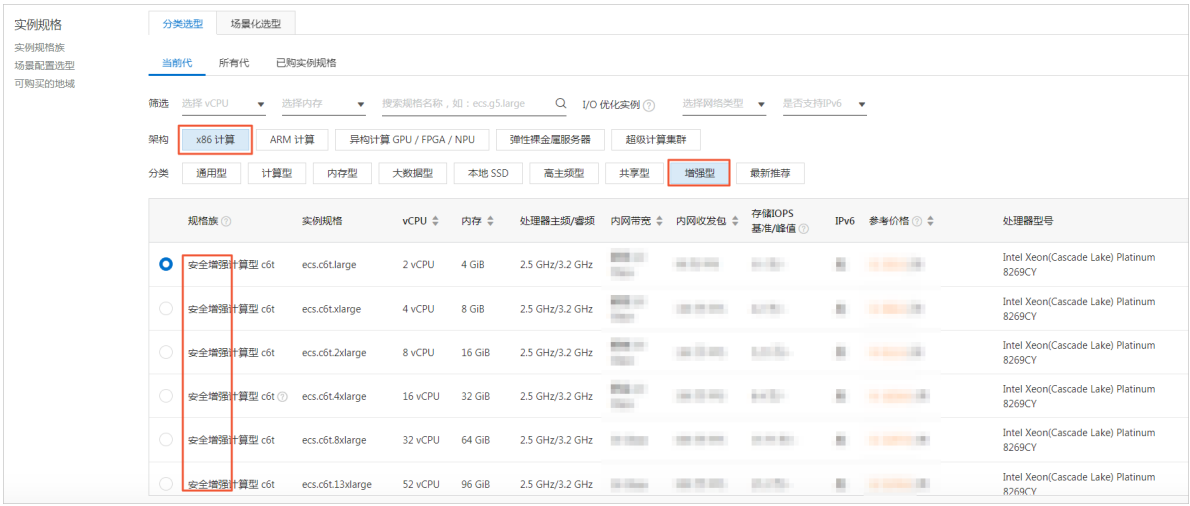
- 开通密钥管理服务。

如果您需要加密云服务相关的数据，建议您提前开通密钥管理服务，无需自行研发和运维密码设施即可在云服务中使用数据加密功能，例如在云服务器ECS中使用云盘加密、实例可信启动等功能。具体操作，请参见开通密钥管理服务。

- 为高安全可信要求的业务选择安全增强型实例。

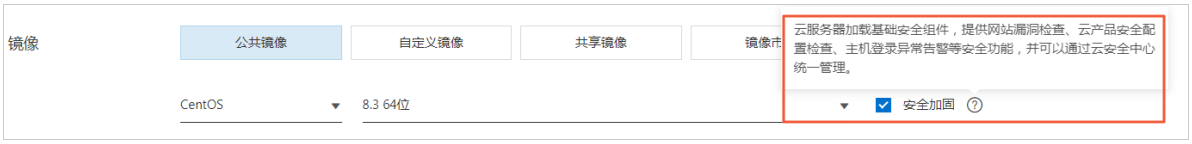
  安全增强型实例基于TPM/TCM芯片提供可信计算能力，保障实例可信启动和实例中隐私数据的安全。更多信息，请参见安全增强型实例概述。

  例如，选择c6t规格。



- 为使用公共镜像的实例启用安全加固。

  启用安全加固的实例在启动时会加载基础安全组件，支持检测异常登录、DDoS攻击、主流漏洞以及云产品安全配置等，并可以通过云安全中心统一管理资产。更多信息，请参见云安全中心免费版简介。



- 启用云盘加密。

  云盘加密功能采用AES-256加密算法，利用了托管在密钥管理服务中的服务密钥，您无需自建和维护密钥管理基础设施即可保护云盘数据的安全。具体操作，请参见加密系统盘和加密数据盘。加密云盘后的效果如下：

  - 系统盘：操作系统内的数据会被自动加密，并在读取数据时自动解密。
  - 数据盘：将加密云盘挂载到实例后，云盘中的静态数据、云盘和实例间传输的数据（不包括操作系统内的数据）、云盘从实例传递到后端存储集群的数据都会被自动加密，并在读取数据时自动解密。此外，从加密云盘创建的所有快照、从加密快照创建的所有云盘也会被自动加密。

  例如，加密随实例添加的数据盘。

- 使用快照进行容灾备份。

  快照是一种便捷高效的数据容灾手段。定期创建快照备份云盘数据后，如果因系统故障、操作失误等原因而导致云盘数据异常或丢失，您可以从最近时间点的快照恢复云盘数据，减少损失。在执行重要操作前，也建议创建快照，避免操作时出现意外情况。

  例如，在创建实例时启用快照服务，每天为所有云盘自动创建快照。

为实例搭建安全的网络环境

搭建网络环境时遵循安全做法，例如网络隔离、网络流量控制等，让实例暴露在有限的范围内，减少被攻击的可能性。

- 使用安全组减少攻击范围。

  安全组是一种虚拟防火墙，您可以基于安全组控制实例的入流量和出流量。使用安全组时建议如下：

  - 将安全组作为白名单使用，即默认拒绝所有访问，通过添加安全组规则设置允许访问的端口范围和授权对象。安全组支持五元组规则，您可以精确控制源IP、源端口、目的IP、目的端口以及传输层协议，更多信息，请参见安全组五元组规则。
  - 添加安全组规则时遵循最小授权原则。例如，开放Linux实例的22端口用于远程登录时，建议仅允许特定的IP访问，而非所有IP（`0.0.0.0/0`）。

    阿里云提供潜在高危安全组检测功能，帮助您及时发现未限制访问的安全组规则。

    如果发现未限制访问的安全组规则，请审视是否需要开放对应的端口，并及时修改过高的授权。例如，如果实例上安装了MySQL数据库服务，不应默认向公网开放3306端口。请将当前安全组规则的改为拒绝所有IP访问，将优先级设为最低，然后遵循最小授权原则添加允许访问的安全组规则。
  - 单个安全组内尽量保持规则简洁。单台实例可以加入多个安全组，单个安全组可以添加多条安全组规则，如果应用在单台实例上的安全组规则过多，会增加管理复杂度并引入风险。
  - 不同类型应用的实例加入不同的安全组，分别维护安全组规则。例如，需要接受公网访问的实例加入同一个安全组，默认拒绝所有访问，然后设置仅暴露对外提供服务的端口（例如80、443等）。同时避免在接受公网访问的实例上提供其他服务，例如MySQL、Redis等，建议将内部服务部署在不接受公网访问的实例上，并加入单独的安全组。
  - 合理利用普通安全组的网络连通策略。普通安全组中的实例默认互通，部分情况下利用默认互通可以降低管理复杂度。例如，已经存在多个安全组，如果为几台需要内网互通的实例添加安全组规则过于复杂，可以为这些实例新建一个安全组。但实例数量较多时，不建议用一个安全组管理所有的实例，会导致该安全组对外的规则管理过于复杂。

    普通安全组也支持设置组内隔离，更多信息，请参见普通安全组内网络隔离。
  - 合理使用普通安全组的组间授权控制内网通信。例如，在分布式应用中，为Web服务和MySQL数据库服务分别创建了安全组SG_Web和SG_Database，您可以在SG_Database中添加安全组规则，授权SG_Web中的实例访问SG_Database中实例的3306端口。

    经典网络类型实例的内网IP经常变化，因此也建议使用安全组间授权，而非基于CIDR网段或内网IP授权。
  - 避免直接修改线上环境使用的安全组。修改安全组设置后会自动应用于组内所有实例，您可以先克隆一个安全组并在测试环境调试，确保修改后实例间通信正常。
  - 合理定义安全组名称、标签等，方便快速识别安全组的用途，在管理较多安全组时更加清晰。关于如何创建标签，请参见创建或绑定标签。

更多安全组设置案例和实践建议，请参见：

- 安全组应用案例ECS安全组配置操作指南
- ECS安全组实践（一）
- ECS安全组实践（二）
- ECS安全组实践（三）

- 使用专有网络隔离企业内部不同安全等级的服务。

  专有网络之间通过隧道技术实现逻辑上彻底隔离，您可以基于阿里云专有网络实现网络隔离。使用专有网络时建议如下：

  - 将需要严格隔离的业务系统部署在不同的专有网络中，例如生产环境和测试环境。
  - 在专有网络内使用交换机划分子网，管理访问策略不同的服务，例如将Web服务部署在提供公网访问能力的子网中、将数据库服务部署在对外完全隔离的子网中。

  更多结合业务规划网络的建议，请参见网络规划。

- 合理使用跳板机或堡垒机防御内外部入侵。

  在专有网络中，建议为用作跳板机的实例创建专用的虚拟交换机，通过分配EIP或配置NAT端口转发表获取公网访问能力，同时通过安全组控制访问。示例如下：

  i. 为跳板机创建专用的安全组SG_Bridge，仅授权访问必要的端口（例如Linux实例的22端口、Windows实例的3389端口）并将授权对象限制为特定的IP或CIDR网段，降低跳板机被未授权登录的概率。
  ii. 将跳板机加入到安全组SG_Bridge中。
  iii. 配置安全组间访问规则，让跳板机可以访问其他安全组中的实例。

  例如，在安全组SG_Current中添加安全组规则，授权对象为安全组SG_Bridge，限制通过特定的协议访问特定的端口。

  > **说明** 通过跳板机登录其他实例时，建议优先使用SSH密钥对。更多信息，请参见SSH密钥对概述。

  跳板机可以在一定程度上增强安全性，但权限仍然较大而且不易审计操作行为。您可以使用更加安全的堡垒机，满足运维工作对权限受控、操作审计、安全合规的要求。阿里云也提供了堡垒机产品，更多信息，请参见什么是堡垒机。

- 仅为必须的实例提供公网访问能力。

  通过合理的方式提供公网访问能力，可以简化访问管理并减少受到外部攻击的风险。建议如下：

  - 大多数分布式应用包括不同的分层和分组，避免为不提供公网访问的实例分配公网IP。如果有多台实例提供公网访问，建议使用负载均衡服务分发公网流量，提升安全性和可用性，避免在公网环境暴露过多实例和因实例的单点故障影响访问。更多信息，请参见什么是传统型负载均衡CLB。
  - 如果专有网络中未分配公网IP的实例只需要访问公网，优先使用NAT网关的SNAT功能提供代理服务，避免因为只需访问公网就将实例直接暴露在公网环境。创建SNAT条目时指定实例或交换机提供公网访问能力，具体操作，请参见创建和管理SNAT条目。

使用云安全产品构建安全防御体系

阿里云提供全面的安全产品和服务，帮助您全面提升云上资产在各种场景下的安全性。

- 使用阿里云DDoS防护服务抵御网络流量攻击。

  DDoS攻击指将多台计算机联合起来作为攻击平台，通过远程连接利用恶意程序，对一个或多个目标发起DDoS攻击，消耗目标服务器性能或网络带宽，从而造成服务器无法正常地提供服务。

阿里云提供DDoS原生防护、DDoS高防等产品，其中DDoS原生防护直接为阿里云公网IP资源（包括云服务器ECS、负载均衡、Web应用防火墙和弹性公网IP）提升DDoS攻击防御能力，适用于资源部署在阿里云上的业务。当流量超出DDoS原生防护的默认清洗阈值后，自动触发流量清洗，实现DDoS攻击防护。您也可以按需自定义清洗阈值，具体操作，请参见设置流量清洗阈值。

DDoS原生防护基础版免费提供不超过5 Gbps的DDoS防护能力，默认开启无需购买。如果您需要更高的防护能力，请购买DDoS防护收费服务，更多信息，请参见阿里云DDoS防护产品介绍。

- 接入阿里云云安全中心防御系统安全漏洞。

  云安全中心免费为ECS实例提供基础的安全加固能力，支持检测异常登录、DDoS攻击、主流漏洞以及云产品安全配置等。更多信息，请参见云安全中心免费版简介。

  云安全中心免费版仅支持检测风险，但不支持处理风险。如需修复漏洞、主动防御等功能，请前往云安全中心控制台购买付费版。

  除免费版的基础安全加固能力外，云安全中心付费版支持更丰富的功能。例如：

  - 漏洞修复：一键修复Linux软件漏洞、Windows系统漏洞等漏洞。漏洞是长期存在的安全风险，云安全中心可以为您解决漏洞发现不及时、修复效率低等问题。
  - 病毒防御：针对病毒提供扫描、告警、深度查杀和数据备份的能力，有效防御病毒入侵您的服务器。
  - 安全告警：针对网页防篡改、进程异常、网站后门、异常登录、恶意进程等威胁提供全面的安全告警类型检测，帮助您及时发现资产中的安全威胁。

  详细的云安全中心功能特性列表，请参见云安全中心功能特性。

- 购买阿里云Web应用防火墙防御应用安全漏洞。

  Web应用防火墙可以有效识别Web业务流量的恶意特征，在对流量进行清洗和过滤后，将正常、安全的流量返回给服务器，避免网站服务器被恶意入侵导致服务器性能异常等问题，保障网站的业务安全和数据安全。

  使用Web应用防火墙时，无需安装任何软硬件或调整路由配置，即可针对性防护常见Web应用攻击、缓解恶意CC攻击等，提高网站安全性。接入Web应用防火墙的具体步骤，请参见Web应用防火墙快速入门。

  在DDoS防护、云安全中心安全加固的基础上，针对网站使用Web应用防火墙可以进一步增强防护能力，全面地提高业务安全性。

实例操作系统内安全配置

操作系统内安全配置是一台实例安全的最后一道屏障，配置得当可以有效降低被入侵的风险。

- 提升登录配置的安全性。
  - Linux实例：
    - 配置仅允许使用SSH密钥对登录Linux实例。SSH密钥对通过加密算法生成一对密钥，默认采用RSA 2048位的加密方式，相比密码更加安全和便捷。关于SSH密钥对的特性和操作介绍，请参见SSH密钥对概述、通过密钥认证登录Linux实例。
    - 日常不使用root用户登录Linux实例，使用其他用户作为管理员。如果该用户执行需要管理员权限的操作，可以通过sudo命令提权。
  - Windows实例：使用强密码，8~30个字符，必须至少同时包含大写字母、小写字母、数字、特殊字符（`()`~!@#$%^&*_-+=|{}[]:;'<>,.?/`）中的三项，建议包含特殊字符。使用密码登录实例时，建议定期更换密码。
- 保护服务端口。

服务器在提供服务时需要开启服务端口，开启的服务端口越多，潜在风险越大。建议只对外开启必要的服务端口，将服务默认的端口号修改为更高的端口号（大于30000），并通过防火墙、安全组等手段控制对端口访问。修改服务器默认远程端口的具体操作，请参见修改服务器默认远程端口。

例如，尽量只在内网环境中访问数据库服务，避免数据库服务暴露在公网环境。如果必须要从公网环境访问数据库服务，将默认端口号（例如，MySQL数据库为3306）修改为更高的端口号，并授权特定的IP访问。

- 避免使用弱口令。

  使用弱口令容易被猜到或破解，然后非法登录服务器窃取数据或破坏服务器。建议您设置复杂的密码并定期修改密码。

使用服务时遵循安全做法

除各类安全产品和配置外，在部署完成后使用服务时也需要遵循安全做法，避免泄露AccessKey、密钥、账号密码等机密信息，并使用审计类功能跟踪使用情况。

- 妥善保管和使用机密信息。
  - 阿里云AccessKey相当于调用云服务API时的登录密码，是访问内部资源时重要的身份凭证。建议如下：
    - 使用RAM用户的AccessKey，而非阿里云账号的AccessKey，并在为RAM用户授权时遵守最小权限原则，避免因泄露AccessKey威胁账号下所有资源的安全。
    - 不要在代码中直接写入AccessKey，避免不慎随代码泄露。
    - 定期轮换AccessKey，保证即使不慎泄露旧AccessKey也不会影响线上业务。
    - 定期吊销不再使用的AccessKey。
    - 使用操作审计功能，并将操作日志保存到SLS Logstore或OSS存储空间中。
    - 关注云安全中心的AccessKey泄露检查通知。云安全中心默认为用户开启AccessKey泄露检查功能，可以精准检测在Github上泄漏的AccessKey并通知用户及早响应，尽可能减少负面影响。
  - 密钥、账号密码安全建议如下：
    - 不同平台间使用不同的密钥、账号密码，避免不慎泄露后影响多个平台中资源的安全。
    - 实例上不同用户间避免共享密钥、账号密码。
    - 用途保持单一，例如勿将远程连接实例的密钥用于其他场景。
  - 使用密钥管理服务安全托管机密信息，避免明文存储。

  更多信息，请参见AK和账密防泄漏最佳实践。

- 数据传输加密。

  在实例和客户端之间传输的敏感数据时使用加密协议（例如TLS1.2及以上版本），并配置安全组和操作系统防火墙，确保实例和敏感远程网络服务之间仅允许通过加密连接通信。

- 使用操作审计功能。

  操作审计可以记录账号的操作事件，并将记录文件保存到SLS Logstore或OSS存储空间中，供您进行安全分析、合规审计和资源变更跟踪。具体操作，请参见创建单账号跟踪。操作审计的应用示例如下：
  - 分析登录时间、登录IP、是否使用多因素认证MFA登录等信息，判断账号是否存在异常登录等安全问题。
  - 如果组织内有多名成员，并使用了访问控制RAM管理成员的身份，获取每个成员的详细操作记录，满足组织合规性审计需要。
  - 在资源状态出现异常变更时，例如一台实例异常停机，可以通过操作日志查找操作人、操作时间、发起操作的IP地址等信息，定位和排查问题。

2.安全组
2.1. 安全组概述

安全组是一种虚拟防火墙，用于控制安全组内ECS实例的入流量和出流量，从而提高ECS实例的安全性。安全组具备状态检测和数据包过滤能力，您可以基于安全组的特性和安全组规则的配置在云端划分安全域。

安全组和安全组规则

安全组分为普通安全组和企业安全组。企业安全组面向企业级场景，可以容纳更多的实例、弹性网卡和私网IP，而且访问策略更加严格。

- 实例加入安全组的规则如下：
  - 实例至少加入一个安全组，可以同时加入多个安全组。
  - 实例上挂载的弹性网卡中，辅助网卡可以加入和实例不同的安全组。
  - 实例不支持同时加入普通安全组和企业安全组。
- 安全组在未添加安全组规则时，自身已经具有控制出入流量的一些特性。在这些特性基础上，您可以继续新增、修改安全组规则更精细地控制出入流量。新增、修改安全组规则后，会自动应用于安全组内所有实例。安全组规则支持针对IP地址、CIDR地址块、其他安全组、前缀列表授权。更多信息，请参见添加安全组规则。
- 在控制台创建安全组时，系统会自动添加默认规则，您可以根据需要维护这些规则。

> **说明**
>
> - 调用API创建安全组时，系统不会自动添加默认规则。
> - 安全组为有状态应用。一个有状态的会话连接中，会话的最长保持时长是910秒。允许访问并建立会话后，安全组会默认放行同一会话中的通信。例如，在会话期内，如果连接的数据包在入方向是允许的，则在出方向也是允许的。

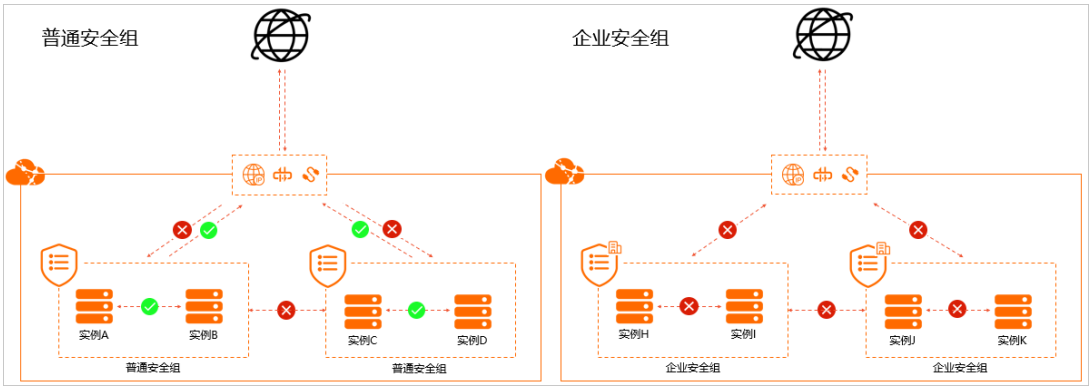
普通安全组和企业安全组的对比差异如下表所示。

对比项	普通安全组	企业安全组
支持的网络类型	经典网络和VPC网络	VPC网络
支持所有实例规格	是	否，仅支持VPC网络类型的实例规格
经典网络下，能容纳的私网IP地址数量	1,000①	不支持经典网络
VPC网络下，能容纳的私网IP地址数量	2,000②，支持自助申请提高到6,000 • 申请方法：在配额中心找到**专有网络普通安全组内的私网IP地址数量上限**配额项进行申请。具体操作，请参见创建配额提升申请。 • 支持的地域：目前该功能正在按地域陆续发布中，支持的地域请参见提高VPC网络普通安全组组内IP地址上限，目前已经在哪些地域发布支持？。	65,536③

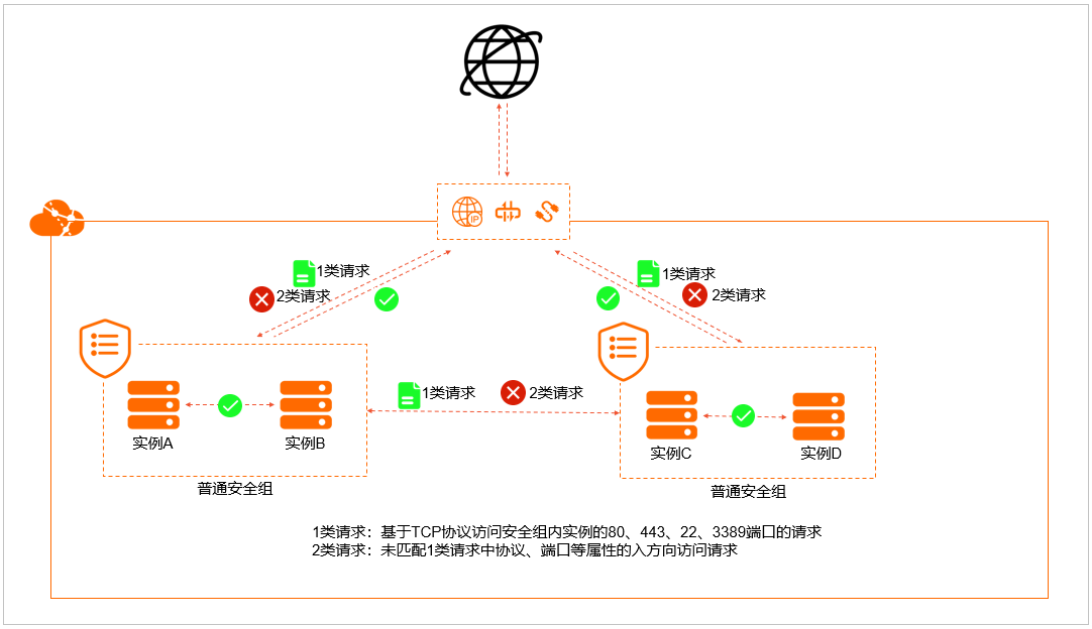
对比项	普通安全组	企业安全组
支持添加允许（或拒绝）访问的安全组规则	是	是
支持设置规则优先级	是	是
支持作为安全组规则的授权对象，授权给其他安全组	是	否
未添加任何安全组规则时，组内实例网络的互通策略	• 同一普通安全组内的实例及弹性网卡之间内网互通，且互通的优先级高于其他任何自定义规则。 • 不同普通安全组内的实例及弹性网卡之间内网隔离。 • 默认拒绝所有入方向的访问请求。 普通安全组未添加安全组规则时，允许和拒绝的访问请求如安全组控制访问请求示意图（未添加安全组规则）所示。	• 同一企业安全组内的实例及弹性网卡之间内网隔离。 • 不同企业安全组内的实例及弹性网卡之间内网隔离。 • 默认拒绝所有入方向和出方向的访问请求。 企业安全组未添加安全组规则时，允许和拒绝访问请求如安全组控制访问请求示意图（未添加安全组规则）所示。
控制台创建安全组时，系统默认添加的规则	• 入方向：5条入方向安全组规则，即针对TCP协议允许所有IP访问HTTP（80）、HTTPS（443）、SSH（22）、RDP（3389）端口，并针对ICMP（IPv4）协议允许所有IP访问所有端口。 • 出方向：无。 如果在控制台创建普通安全组时保留了上述默认规则，允许和拒绝的访问请求如普通安全组控制访问请求示意图（保留默认规则）所示。	• 入方向：5条入方向安全组规则，即针对TCP协议允许所有IP访问HTTP（80）、HTTPS（443）、SSH（22）、RDP（3389）端口，并针对ICMP（IPv4）协议允许所有IP访问所有端口。 • 出方向：1条出方向安全组规则，即针对所有协议允许所有IP访问所有端口，避免引起网络连通性问题。 如果在控制台创建企业安全组时保留了上述默认规则，允许和拒绝的访问请求如企业安全组控制访问请求示意图（保留默认规则）所示。

说明：关于①、②和③的限制说明，请参见安全组使用限制。

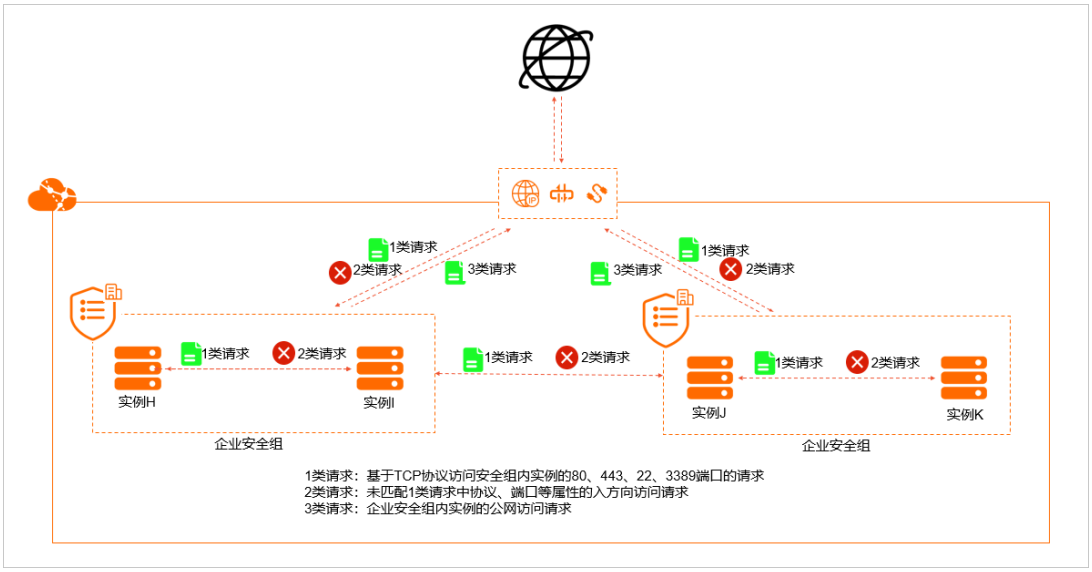
安全组控制访问请求示意图（未添加安全组规则）



普通安全组控制访问请求示意图（保留默认规则）



企业安全组控制访问请求示意图（保留默认规则）



如果一台实例加入了多个安全组，则所有安全组的安全组规则均应用于该实例。在检测到访问请求时，系统会逐一检查适用于实例的安全组规则，根据安全组规则的协议、端口、优先级等属性进行判断，匹配到允许访问的安全组规则时才会建立会话。更多安全组规则的属性说明和示例，请参见安全组规则概述。

安全组使用指导

使用安全组控制实例流量的典型使用流程如下：

1. 创建安全组。
2. 添加安全组规则。
3. 将实例加入安全组。
4. 按需管理已有安全组和安全组规则。

使用安全组控制辅助网卡流量的典型使用流程如下：

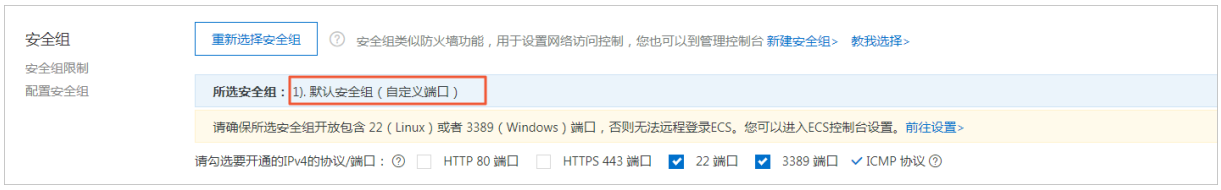
1. 创建安全组。

2. 添加安全组规则。
3. 将辅助网卡加入安全组。
4. 将辅助网卡绑定至实例。
5. 按需管理已有安全组和安全组规则。

关于安全组的具体操作和应用案例，请参见安全组操作导航和安全组应用案例ECS安全组配置操作指南。

默认安全组

实例至少需要加入一个安全组。通过ECS管理控制台创建实例时，如果您还未在所选地域创建安全组，可以使用默认安全组。系统会在创建实例的同时创建一个安全组，网络类型和实例一致。默认安全组的安全组类型为普通安全组，安全组规则配置如下图所示。



默认安全组规则的效果如下：

- 规则优先级：100。

  > **说明** 2020年05月27日以前系统创建的默认安全组规则的优先级为110。

- 针对TCP协议允许所有IP访问SSH(22)、RDP(3389)端口。
- 针对ICMP(IPv4)协议允许所有IP访问所有端口。
- 如果选中**HTTP 80端口**和**HTTPS 443端口**，还会针对TCP协议允许所有IP访问HTTP(80)、HTTPS(443)端口。

安全组托管模式

部分其他云产品（例如云防火墙、NAT网关等）也会使用安全组的能力。为了保障云产品的服务可用，并防止您误操作资源，这些云产品会自动创建托管模式的安全组。该类安全组由对应的云产品管理，您只有查看权限，没有操作权限。更多信息，请参见托管安全组。

实践建议

- 将安全组作为白名单使用，即默认拒绝所有访问，通过添加安全组规则设置允许访问的端口范围和授权对象。
- 添加安全组规则时遵循最小授权原则。例如，开放Linux实例的22端口用于远程登录时，建议仅允许特定的IP访问，而非所有IP（`0.0.0.0/0`）。
- 单个安全组内尽量保持规则简洁。单台实例可以加入多个安全组，单个安全组可以添加多条安全组规则，如果应用在单台实例上的安全组规则过多，会增加管理复杂度并引入风险。
- 不同类型应用的实例加入不同的安全组，分别维护安全组规则。例如，需要接受公网访问的实例加入同一个安全组，默认拒绝所有访问，然后设置仅暴露对外提供服务的端口（例如80、443等）。同时避免在接受公网访问的实例上提供其他服务，例如MySQL、Redis等，建议将内部服务部署在不接受公网访问的实例上，并加入单独的安全组。
- 避免直接修改线上环境使用的安全组。修改安全组设置后会自动应用于组内所有实例，您可以先克隆一个安全组并在测试环境调试，确保修改后实例间通信正常。
- 合理定义安全组名称、标签等，方便快速识别安全组的用途，在管理较多安全组时更加清晰。

合理使用安全组可以有效提高实例的安全性，但提高实例安全性是一项系统的工作，您还可以结合更多其他做法。更多信息，请参见安全最佳实践。

2.2. 托管安全组

为了保障云产品的服务可用，并防止您误操作资源。当您使用需要创建安全组的云产品时，云产品系统将选择创建托管模式的安全组，即托管安全组。本文主要介绍托管安全组及相关权限。

背景信息

托管模式下的安全组称为托管安全组。该模式是为了解决部分云产品（例如：云防火墙、NAT网关等）的安全组操作权限控制问题。该类安全组由云产品系统管理，您只有查看权限，没有操作权限。详细说明如下：

> **说明** 创建托管安全组的方式是阿里云云产品通过阿里云临时安全令牌（Security Token Service，STS）授权您的账号的RAM角色自动进行的。关于STS的详细信息，请参见什么是STS。

- 通过云产品控制台，您不能操作托管安全组，仅能在控制台界面查看托管安全组的相关信息。
- 通过OpenAPI访问托管安全组，您仅能调用查询接口。如果您调用操作安全组相关的接口，将提示您该安全组为云产品系统管理的安全组，您无法操作，即返回包含错误码 `InvalidOperation.ResourceManagedByCloudProduct` 的错误信息。具体权限，请参见托管安全组的OpenAPI权限说明。

您可以通过调用DescribeSecurityGroups接口，查看返回值参数 `ServiceManaged` 和 `ServiceID` ，确认相关的安全组是否为托管安全组。

托管安全组的OpenAPI权限说明

API	操作	您的阿里云账号	创建托管安全的云产品系统
AuthorizeSecurityGroup	• 增加安全组入方向规则 • 入方向授权托管安全组的访问权限	不可操作	可以操作
AuthorizeSecurityGroupEgress	• 增加安全组出方向规则 • 出方向授权托管安全组的访问权限	不可操作	可以操作
RevokeSecurityGroup	删除安全组入方向规则	不可操作	可以操作
RevokeSecurityGroupEgress	删除安全组出方向规则	不可操作	可以操作
JoinSecurityGroup	加入安全组	不可操作	可以操作
LeaveSecurityGroup	离开安全组	不可操作	可以操作
DeleteSecurityGroup	删除安全组	不可操作	可以操作
ModifySecurityGroupAttribute	修改安全组	不可操作	可以操作
ModifySecurityGroupRule	修改安全组入方向规则描述	不可操作	可以操作

API	操作	您的阿里云账号	创建托管安全的云产品系统
ModifySecurityGroupEgressRule	修改安全组出方向规则描述	不可操作	可以操作
ModifySecurityGroupPolicy	修改安全组策略	不可操作	可以操作
DescribeSecurityGroupAttribute	查询安全组规则	可以操作	可以操作
DescribeSecurityGroups	查询安全组列表	可以操作	可以操作
DescribeSecurityGroupReferences	查询安全组和其他哪些安全组有安全组级别的授权行为	可以操作	可以操作
CreateNetworkInterface	创建弹性网卡	不可操作	可以操作
ModifyNetworkInterfaceAttribute	修改弹性网卡	不可操作	可以操作
RunInstances	创建实例	不可操作	可以操作
CreateInstance	创建实例	不可操作	可以操作
ModifyInstanceAttribute	修改实例的安全组	不可操作	可以操作

2.3. 安全组应用案例

本文针对网站提供Web服务、远程连接实例等常见场景，介绍如何基于安全组的特性配置安全组规则。

背景信息

本文中安全组规则示例的说明如下：

- 均针对网络类型为专有网络的安全组，一条安全组规则同时适用于控制公网和内网访问。对于网络类型为经典网络的安全组，请注意为控制公网和内网访问分别创建安全组规则。
- 均针对典型应用的默认端口。应用通过服务器的端口对外提供服务，更多信息，请参见典型应用的常用端口。

网站提供Web服务

安全组默认拒绝所有入方向访问。如果您在实例上搭建对外提供Web服务的网站，需要允许访问相应服务的端口，例如HTTP(80)、HTTPS(443)，安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：80/80	源：0.0.0.0/0
入方向	允许	1	自定义TCP	目的：443/443	源：0.0.0.0/0

> **说明** 如果添加安全组规则后仍无法访问网站，排查思路请参见检查TCP 80端口是否正常工作。

从本地服务器远程连接实例

安全组默认拒绝所有入方向访问。从本地服务器远程连接实例前，需根据连接方式允许访问相应服务的端口，例如通过SSH远程连接Linux实例时允许访问SSH(22)，通过RDP远程连接Windows实例时允许访问RDP(3389)，安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：22/22	源：0.0.0.0/0
入方向	允许	1	自定义TCP	目的：3389/3389	源：0.0.0.0/0

说明 `0.0.0.0/0` 为允许所有IP远程连接实例。为安全起见，建议您在实际业务中将授权对象设置为特定的IP，遵循最小授权原则。

使用阿里云Workbench远程连接实例时，允许访问特定的服务器即可，安全组规则示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：22/22	源：161.117.90.22/32
入方向	允许	1	自定义TCP	目的：3389/3389	源：161.117.90.22/32

说明 关于使用Workbench连接经典网络实例的安全组规则说明，请参见Linux实例相关安全组规则详情和Windows实例相关安全组规则详情。

不同安全组的实例内网互通

不同安全组之间的实例默认内网隔离。在同一个专有网络中，如果在实例间进行数据共享等操作，例如安全组A的实例都需要通过FTP查看安全组B的实例中的共享文件，您可以通过授权安全组访问实现内网互通，比授权单个IP地址或者CIDR地址块更加便捷。

说明 如果实例分属于不同的专有网络，则不能通过安全组实现内网互通。您可以使用云企业网连接不同专有网络之间的实例，更多信息，请参见云企业网快速入门。

安全组A和安全组B属于同一账号时，授权对象填写安全组ID即可，安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：21/21	源：sg-bp1hv6wvmegs036****

说明 安全组ID仅为示例，请按实际情况替换。

安全组A和安全组B属于不同账号时，授权对象需要填写阿里云账号ID和安全组ID，安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：21/21	源：160998252992****/sg-bp174yoe2ib1sqj5****

> **说明** 阿里云账号ID和安全组ID仅为示例，请按实际情况替换。

提供数据库访问

如果您在实例上部署了数据库，需要允许其他实例通过内网获取数据，请根据数据库类型允许访问相应服务的端口，例如MySQL (3306)、Oracle(1521)、MS SQL(1433)、PostgreSQL(5432)、Redis(6379)，安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：3306/3306	源：172.16.XX.XX
入方向	允许	1	自定义TCP	目的：1521/1521	源：192.168.XX.XX
入方向	允许	1	自定义TCP	目的：1433/1433	源：192.168.XX.XX/16
入方向	允许	1	自定义TCP	目的：5432/5432	源：sg-bp1hv6wvmegs036****
入方向	允许	1	自定义TCP	目的：6379/6379	源：160998252992****/sg-bp174yoe2ib1sqj5****

> **说明** IP地址、CIDR地址块、阿里云账号ID和安全组ID仅为示例，请按实际情况替换。

ping实例

ICMP协议用于传递控制消息，允许基于ICMP协议的访问后才能完成一些测试操作，例如在客户端执行ping命令测试网络可达性，安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	全部ICMP(IPv4)	目的：-1/-1	源：0.0.0.0/0

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	全部ICMP(IPv6)	目的：-1/-1	源：::/0

限制实例访问外部网站

普通安全组默认允许所有出方向访问。如果需要限制实例只能访问指定网站，可以将安全组作为白名单使用，设置默认拒绝所有出方向访问，然后仅允许访问指定网站的IP。设置时您需要注意：

- 系统基于协议、端口、授权对象匹配到多条安全组规则后，会继续通过优先级和授权策略来判定最终生效的安全组规则，最终结果为允许访问时才建立会话。
- 安全组规则优先级的数值越小，代表优先级越高。相同优先级的情况下，如果两条安全组规则只有授权策略不同，则拒绝策略的安全组规则生效。因此拒绝策略的优先级应低于允许策略的优先级，这样允许策略的安全组规则才能生效，以实现出方向访问指定网站的IP。

安全组规则的配置示例如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
出方向	拒绝	2	全部	目的：-1/-1	目的：0.0.0.0/0
出方向	允许	1	自定义TCP	目的：80/80	目的：47.96.XX.XX
出方向	允许	1	自定义TCP	目的：443/443	目的：121.199.XX.XX

> **说明** 网站的IP仅为示例，请按实际情况替换。

添加安全组规则后，您可以登录实例进行测试，例如执行ping命令。如果实例只能访问指定的IP地址，说明安全组规则已经生效。

2.4. 典型应用的常用端口

通过了解典型应用的默认端口，您可以更准确地添加或修改安全组规则。

背景信息

添加安全组规则时，您必须指定通信端口或端口范围，然后安全组根据允许或拒绝策略决定是否转发数据到ECS实例。例如，使用Xshell客户端远程连接ECS实例时，当安全组检测到从公网或内网有SSH请求，会同时检查入方向上发送请求的设备的IP地址是否在允许放行的安全组规则中、22端口是否开启，只有匹配到的安全组规则允许放行该请求时，方才建立数据通信。

> **说明** 部分运营商判断端口25、135、139、444、445、5800、5900等为高危端口，并默认屏蔽。即使您添加的安全组规则放行了这些端口，在受限地区仍无法访问。建议您修改为其它非高危端口承载业务。

更多关于Windows Server系统应用的端口说明，请参见 *微软文档* Windows服务器系统的服务概述和网络端口要求。

端口列表

参见下表查看常用端口的使用说明。

端口	服务	说明
21	FTP	FTP服务所开放的端口，用于上传、下载文件。
22	SSH	SSH端口，用于通过命令行模式或远程连接软件（例如PuTTY、Xshell、SecureCRT等）连接Linux实例。详情请参见通过密码认证登录Linux实例。
23	Telnet	Telnet端口，用于Telnet远程登录ECS实例。
25	SMTP	SMTP服务所开放的端口，用于发送邮件。 基于安全考虑，ECS实例25端口默认受限，如需解封，请参见TCP 25端口控制台解封申请。
53	DNS	用于域名解析服务器（Domain Name Server，简称DNS）协议。 如果在安全组出方向实行白名单方式，需要放行此端口才能实现域名解析。
80	HTTP	用于HTTP服务提供访问功能，例如，IIS、Apache、Nginx等服务。 如何排查80端口故障，请参见检查TCP 80端口是否正常工作。
110	POP3	用于POP3协议，POP3是电子邮件收发的协议。
143	IMAP	用于IMAP（Internet Message Access Protocol）协议，IMAP是用于电子邮件的接收的协议。
443	HTTPS	用于HTTPS服务提供访问功能。HTTPS是一种能提供加密和通过安全端口传输的一种协议。
1433	SQL Server	SQL Server的TCP端口，用于供SQL Server对外提供服务。
1434	SQL Server	SQL Server的UDP端口，用于返回SQL Server使用了哪个TCP/IP端口。
1521	Oracle	Oracle通信端口，ECS实例上部署了Oracle SQL需要放行的端口。
3306	MySQL	MySQL数据库对外提供服务的端口。
3389	Windows Server Remote Desktop Services	Windows Server Remote Desktop Services（远程桌面服务）端口，可以通过这个端口使用软件连接Windows实例。详情请参见通过密码认证登录Windows实例。
8080	代理端口	同80端口一样，8080端口常用于WWW代理服务，实现网页浏览。如果您使用了8080端口，访问网站或使用代理服务器时，需要在IP地址后面加上 `:8080` 。安装Apache Tomcat服务后，默认服务端口为8080。
137、138、139	NetBIOS协议	• 137、138为UDP端口，通过网上邻居传输文件时使用的端口。 • 139通过这个端口进入的连接试图获得NetBIOS/SMB服务。 NetBIOS协议常被用于Windows文件、打印机共享和Samba。

常用端口典型应用

下表为云服务器ECS的部分端口通信场景，更多场景举例请参见安全组应用案例ECS安全组配置操作指南。

使用场景	网络类型	方向	策略	协议	端口范围	对象类型	授权对象	优先级
SSH远程连接Linux实例	专有网络VPC	入方向	允许	自定义TCP	SSH(22)	地址段访问	0.0.0.0/0	1
	经典网络	公网入方向						
RDP远程连接Windows实例	专有网络VPC	入方向	允许	自定义TCP	RDP(3389)	地址段访问	0.0.0.0/0	1
	经典网络	公网入方向						
公网Ping ECS实例	专有网络VPC	入方向	允许	全部ICMP	-1/-1	地址段访问或安全组访问	根据授权类型填写	1
	经典网络	公网入方向						
ECS实例作Web服务器	专有网络VPC	入方向	允许	自定义TCP	HTTP(80)	地址段访问	0.0.0.0/0	1
	经典网络	公网入方向						
使用FTP上传或下载文件	专有网络VPC	入方向	允许	自定义TCP	20/21	地址段访问	指定IP段	1
	经典网络	公网入方向						

2.5. 安全组操作导航

本文介绍安全组的使用操作，您可以通过ECS控制台或API使用安全组。

控制台操作

在ECS控制台上使用安全组的相关操作如下表所示。

操作任务	说明	相关文档
创建安全组	您可以自行创建一个安全组。	创建安全组
添加安全组规则	创建安全组后，您可以自定义添加或修改安全组规则，控制出入方向的网络访问。	添加安全组规则

操作任务	说明	相关文档
ECS实例加入到安全组	您可以将实例加入到安全组中来统一管理网络访问策略。一台ECS实例不能同时加入普通安全组和企业安全组。 如果ECS实例已经在普通安全组中，可通过替换安全组加入到企业安全组中。	• ECS实例加入安全组 • 替换ECS实例的安全组
弹性网卡加入到安全组	您可以将弹性网卡加入到安全组中来统一管理网络访问策略。如果弹性网卡在普通安全组中，可通过修改弹性网卡加入到企业安全组中。	修改弹性网卡
将弹性网卡绑定到ECS实例	ECS实例绑定弹性网卡后，安全组规则即开始生效。	绑定弹性网卡
管理安全组	您可以对安全组执行查询、修改、克隆、移出实例、删除等管理操作。	• 查询安全组 • 修改安全组 • 克隆安全组 • 移出安全组 • 删除安全组
管理安全组规则	安全组规则支持查询、修改、还原、导出、导入和删除操作。	• 查询安全组规则 • 修改安全组规则 • 还原安全组规则 • 导出安全组规则 • 导入安全组规则 • 删除安全组规则

API操作

您可以调用以下API使用安全组。

API	说明
CreateSecurityGroup	自行创建一个安全组。 **说明** 在创建企业安全组之前，您需要确保有可用的专有网络VPC与虚拟交换机。
AuthorizeSecurityGroup	添加一条入方向上的安全组规则，指定安全组入方向的访问权限，允许或者拒绝其他设备发送入方向流量到安全组里的实例。
AuthorizeSecurityGroupEgress	添加一条出方向上的安全组规则， 指定安全组出方向的访问权限，允许或者拒绝安全组里的实例发送出方向流量到其他设备。
JoinSecurityGroup	将一台ECS实例加入到指定的安全组中。

API	说明
ModifyInstanceAttribute	切换安全组类型。如果ECS实例处于普通安全组中，通过ModifyInstanceAttribute可以切换为企业安全组。 说明 切换安全组类型前，您需要充分了解两种安全组规则的配置区别，避免影响实例网络。
ModifyNetworkInterfaceAttribute	修改弹性网卡所属安全组。如果弹性网卡在普通安全组中，通过ModifyNetworkInterfaceAttribute可以将弹性网卡加入到企业安全组。
AttachNetworkInterface	将已加入安全组的弹性网卡挂载到专有网络VPC类型的ECS实例上。
DescribeSecurityGroups	查看您在当前地域下已创建的安全组信息。

2.6. 创建安全组

安全组是ECS实例的虚拟防火墙，用于设置单个或多个ECS实例的网络访问控制，每台ECS实例至少需要属于一个安全组。本文介绍如何在ECS控制台上创建一个安全组并设置安全组规则。

前提条件

如果您要创建专有网络VPC类型安全组，请确认您已经有可用的专有网络VPC和交换机。更多信息，请参见创建和管理专有网络。

背景信息

在您创建ECS实例时，如果您还未创建过安全组，阿里云会为您创建一个默认安全组。默认安全组中的默认规则如下所示：

- 默认开放ICMP协议，用于Ping ECS服务器等操作。
- 默认入方向开放SSH 22端口和RDP 3389端口，用于访问ECS实例。
- 可选入方向开放HTTP 80端口和HTTPS 443端口，如果您使用ECS实例进行建站，需要选中HTTP 80端口和HTTPS 443端口。

如果您希望ECS实例加入自定义的安全组，您可以根据以下操作先自行创建安全组。更多信息，请参见安全组概述。

操作步骤

1. 进入安全组页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**网络与安全 > 安全组**。
   iii. 在顶部菜单栏左上角处，选择地域。
2. 单击**创建安全组**。
3. 在**基本信息**区域，设置安全组的基本信息。

名称	描述
安全组名称	设置安全组名称。
描述	简短地描述安全组，方便后期管理。
网络	设置安全组的网络类型。 ○ 如果为专有网络类型安全组，选择已经创建的专有网络VPC。 ○ 如果为经典网络类型安全组，选择**经典网络**。
安全组类型	选择安全组类型。 ○ 普通安全组：适用于集群规模较小，网络连接数适中的用户场景。 ○ 企业级安全组：适用于集群规模较大，对运维效率有更高需求的用户场景。 更多功能差异，请参见安全组概述。
资源组	设置安全组所属的资源组，便于后续分类运维。
标签	设置安全组的标签信息，便于后续分类运维。

4. （可选）在**访问规则**区域，设置安全组规则。

   默认情况下，系统已经为您配置基本的安全组规则。如果您需要自定义其他规则，可以参考以下操作。更多信息，请参见添加安全组规则。

   i. 单击**入方向**或**出方向**等页签，选择安全组规则方向。

网络类型	选择规则方向
专有网络VPC	■ 入方向：同时控制公网和内网入方向。 默认已允许ICMP协议、SSH 22端口、RDP 3389端口、HTTP 80端口和HTTPS 443端口的入方向规则。 ■ 出方向：同时控制公网和内网出方向。 普通安全组默认全允许；企业安全组默认全拒绝。
经典网络	■ 公网入方向：出于安全性考虑，经典网络的公网入方向规则，授权对象优先使用安全组。如果使用IP地址，则只能授权单一IP地址，不能使用CIDR地址块。 ■ 公网出方向：默认全允许。 ■ 入方向：内网入方向，默认已允许ICMP协议、SSH 22端口、RDP 3389端口、HTTP 80端口和HTTPS 443端口的入方向规则。 ■ 出方向：内网出方向，默认全允许。

   ii. 单击**手动添加**。

   iii. 设置自定义的安全组规则。

名称	描述
授权策略	■ **允许**：放行该端口相应的访问请求。 ■ **拒绝**：直接丢弃数据包，不会返回任何回应信息。 如果两个安全组规则其他都相同只有授权策略不同，则**拒绝**授权生效，**允许**策略不生效。
优先级	优先级数值越小，优先级越高，取值范围为1~100。
协议类型	协议类型包括： ■ **全部**：支持全部协议类型。 ■ **自定义TCP**：支持TCP协议。 ■ **自定义UDP**：支持UDP协议。 ■ **全部ICMP（IPv4）**：支持ICMP（IPv4）协议。 ■ **全部ICMP（IPv6）**：支持ICMP（IPv6）协议。 ■ **全部GRE**：支持GRE协议。
端口范围	**协议类型**为**自定义TCP**或**自定义UDP**时，可手动设置端口范围。多个端口范围以英文半角逗号分隔，例如 `22/23,443/443` 。 关于**协议类型**和**端口范围**的更多信息，请参见典型应用的常用端口或者安全组规则中协议和端口之间是什么关系？。

名称	描述
授权对象	支持以下方式设置授权对象。 ■ IP地址 设置单一IP地址，例如192.168.0.100、2408:4321:180:1701:94c7:bc38:3bfa:。 ■ CIDR地址块 设置IP地址段，例如192.168.0.0/24、2408:4321:180:1701:94c7:bc38:3bfa:***/128。关于IP地址与CIDR地址块的更多信息，请参见安全组规则授权对象中的IP地址和CIDR地址块是什么关系？。 ■ 安全组 安全组访问只对内网有效。授权本账号或其他账号下某个安全组中的ECS实例或者弹性网卡访问本安全组中的ECS实例，实现内网互通。 **说明** ■ 企业安全组不支持授权安全组访问。 ■ 每个普通安全组支持授权的安全组个数最多为20。 ■ 本账号授权：填写同账号下的目标安全组ID。如果是专有网络VPC类型的安全组，目的安全组必须在同一个专有网络VPC中。 ■ 跨账号授权：填写目标阿里云账号ID和目标安全组ID（格式为 **目标阿里云账号ID/目标安全组ID** ）。在**账号管理 > 基本资料**里查看阿里云账号ID。 ■ 前缀列表 前缀列表是一些网络前缀（CIDR地址块的简称）的集合，仅支持VPC网络。您选择前缀列表后，这条安全组规则将会对前缀列表中的所有CIDR地址块生效。更多信息，请参见前缀列表概述和创建前缀列表。 选择前缀列表后，前缀列表占用的安全组规则额度以前缀列表的最大条目容量为准。例如，某前缀列表的最大条目容量为100条，即使该前缀列表中实际包含的条目数未达到100条，在安全组引用该前缀列表后，也会占用该安全组100条规则额度。 设置注意事项如下： ■ 支持同时添加多组授权对象，用英文半角逗号（,）隔开，最多支持添加10组授权对象。但是每组授权对象会对应一条规则，例如您同时添加了10组授权对象，会对应生成10条规则。 ■ 如果填写 `0.0.0.0/0` （IPv4）或者 `::/0` （IPv6），表示允许所有IP地址的访问，设置时请务必谨慎。 ■ 出于安全性考虑，经典网络的公网入方向规则，授权对象优先使用安全组。如果使用IP地址，则只能授权单一IP地址，不能使用CIDR地址块。
描述	安全组规则描述信息。

5. 单击**创建安全组**。

执行结果

创建成功后，安全组列表中新增了一个安全组。

后续步骤

- 您可以通过添加安全组规则，允许或禁止安全组内的ECS实例对公网或私网的访问。具体操作，请参见添加安全组规则。
- 每台ECS实例至少属于一个安全组，您可以根据业务需要，将ECS实例加入一个或多个安全组。具体操作，请参见ECS实例加入安全组。
- 关于实例设置安全组后还是无法访问业务的更多信息，请参见为什么我配置安全组后还是无法访问服务？。

相关文档

- CreateSecurityGroup

2.7. 添加安全组规则

您可以通过添加安全组规则，允许或禁止安全组内的ECS实例对公网或私网的访问。

前提条件

添加安全组规则之前，您已经规划好ECS实例需要允许或禁止哪些公网或内网的访问。更多有关安全组规则设置的应用案例，请参见安全组应用案例ECS安全组配置操作指南。

背景信息

安全组负责管理是否放行来自公网或者内网的访问请求。为安全起见，安全组入方向大多采取拒绝访问策略。如果您使用的是默认安全组，则系统会给部分通信端口自动添加安全组规则。

本文内容适用于以下场景：

- 当您的应用需要与ECS实例所在安全组之外的网络相互通信，但请求发起后进入长时间等待状态，您需要优先设置安全组规则。
- 当您在运营应用的过程中发现部分请求来源有恶意攻击行为，您可以添加拒绝访问的安全组规则实行隔离策略。

添加安全组规则之前，请了解以下内容：

- 普通安全组在未添加任何安全组规则之前，出方向允许所有访问，入方向拒绝所有访问。
- 企业安全组在未添加任何安全组规则之前，出方向和入方向都拒绝所有访问。同时不支持授权给其他安全组。
- 安全组规则支持IPv4安全组规则和IPv6安全组规则。
- 每个安全组的入方向规则与出方向规则的总数不能超过200条。
- 普通安全组授权对象为安全组的规则，不能超过20条。

更多信息，请参见安全组概述。

操作步骤

1. 进入安全组页面。
   i. 登录ECS管理控制台。
   ii. 在左侧导航栏，选择**网络与安全 > 安全组**。
   iii. 在顶部菜单栏左上角处，选择地域。
2. 找到目标安全组，在**操作**列中，单击**配置规则**。
3. 在**安全组规则**页面的**访问规则**区域，根据安全组不同的网络类型选择安全组规则的规则方向。

网络类型	选择规则方向
专有网络VPC	○ 入方向：同时控制公网和内网入方向 ○ 出方向：同时控制公网和内网出方向
经典网络	○ 公网入方向 ○ 公网出方向 ○ 入方向：内网入方向 ○ 出方向：内网出方向

4. 添加安全组规则。
   - 方式一：快速添加安全组规则

     适用于快速设置常用的TCP协议规则，您单击**快速添加**后，只需要设置**授权策略**、**授权对象**，并选中一个或多个端口便能完成。
   - 方式二：手动添加安全组规则

     支持自定义配置授权策略、优先级、协议类型等信息。具体操作，如下所示。

     i. 单击**手动添加**。
     ii. 在规则列表中，配置新增的安全组规则。

名称	描述
授权策略	■ **允许**：放行该端口相应的访问请求。 ■ **拒绝**：直接丢弃数据包，不会返回任何回应信息。 如果两个安全组规则其他都相同只有授权策略不同，则**拒绝**授权生效，**允许**策略不生效。
优先级	优先级数值越小，优先级越高，取值范围为1~100。

名称	描述
协议类型	协议类型包括： ■ **全部**：支持全部协议类型。 ■ **自定义TCP**：支持TCP协议。 ■ **自定义UDP**：支持UDP协议。 ■ **全部ICMP（IPv4）**：支持ICMP（IPv4）协议。 ■ **全部ICMP（IPv6）**：支持ICMP（IPv6）协议。 ■ **全部GRE**：支持GRE协议。
端口范围	**协议类型**为**自定义TCP**或**自定义UDP**时，可手动设置端口范围。多个端口范围以英文半角逗号分隔，例如 `22/23,443/443` 。 关于**协议类型**和**端口范围**的更多信息，请参见典型应用的常用端口或者安全组规则中协议和端口之间是什么关系？。

名称	描述
授权对象	支持以下方式设置授权对象。 ■ IP地址 设置单一IP地址，例如192.168.0.100、2408:4321:180:1701:94c7:bc38:3bfa:。 ■ CIDR地址块 设置IP地址段，例如192.168.0.0/24、2408:4321:180:1701:94c7:bc38:3bfa:***/128。关于IP地址与CIDR地址块的更多信息，请参见安全组规则授权对象中的IP地址和CIDR地址块是什么关系？。 ■ 安全组 安全组访问只对内网有效。授权本账号或其他账号下某个安全组中的ECS实例或者弹性网卡访问本安全组中的ECS实例，实现内网互通。 **说明** ■ 企业安全组不支持授权安全组访问。 ■ 每个普通安全组支持授权的安全组个数最多为20。 ■ 本账号授权：填写同账号下的目标安全组ID。如果是专有网络VPC类型的安全组，目的安全组必须在同一个专有网络VPC中。 ■ 跨账号授权：填写目标阿里云账号ID和目标安全组ID（格式为 **目标阿里云账号ID/目标安全组ID** ）。在**账号管理 > 基本资料**里查看阿里云账号ID。 ■ 前缀列表 前缀列表是一些网络前缀（CIDR地址块的简称）的集合，仅支持VPC网络。您选择前缀列表后，这条安全组规则将会对前缀列表中的所有CIDR地址块生效。更多信息，请参见前缀列表概述和创建前缀列表。 选择前缀列表后，前缀列表占用的安全组规则额度以前缀列表的最大条目容量为准。例如，某前缀列表的最大条目容量为100条，即使该前缀列表中实际包含的条目数未达到100条，在安全组引用该前缀列表后，也会占用该安全组100条规则额度。 设置注意事项如下： ■ 支持同时添加多组授权对象，用英文半角逗号（,）隔开，最多支持添加10组授权对象。但是每组授权对象会对应一条规则，例如您同时添加了10组授权对象，会对应生成10条规则。 ■ 如果填写 `0.0.0.0/0` （IPv4）或者 `::/0` （IPv6），表示允许所有IP地址的访问，设置时请务必谨慎。 ■ 出于安全性考虑，经典网络的公网入方向规则，授权对象优先使用安全组。如果使用IP地址，则只能授权单一IP地址，不能使用CIDR地址块。
描述	安全组规则描述信息。

iii. 在规则的**操作**列中，单击**保存**。

执行结果

添加完成后，在安全组规则列表中查看已添加的安全组规则。安全组规则的变更会自动应用到安全组内的ECS实例上，建议您立即测试是否生效。

常见问题

- 关于**协议类型**和**端口范围**的问题，请参见典型应用的常用端口或者安全组规则中协议和端口之间是什么关系？。
- 关于实例设置安全组后还是无法访问业务的问题，请参见为什么我配置安全组后还是无法访问服务？。
- 关于无法访问80端口和TCP 25端口的问题，请参见为什么无法访问80端口？和为什么无法访问TCP 25端口？。
- 关于其他安全组规则的更多问题，请参见安全FAQ。

相关文档

- AuthorizeSecurityGroup
- AuthorizeSecurityGroupEgress

2.8. ECS实例加入安全组

安全组用于设置单台或多台ECS实例的网络访问控制，它是重要的网络安全隔离手段。您可以根据业务需要，将ECS实例加入一个或多个安全组。一台ECS实例至少属于一个安全组，默认情况下，最多不能超过五个安全组。

前提条件

在设置ECS实例加入安全组之前，请确认以下信息：

- 您必须已经成功创建ECS实例。具体操作，请参见使用向导创建实例。
- ECS实例加入安全组时，目标安全组的网络类型与ECS实例的网络类型必须一致。如果网络类型是专有网络，目标安全组与ECS实例必须属于同一个VPC网络。
- 如果ECS实例已加入其他安全组，此次加入的安全组类型必须和其他安全组一致。更多详情，请参见安全组概述。

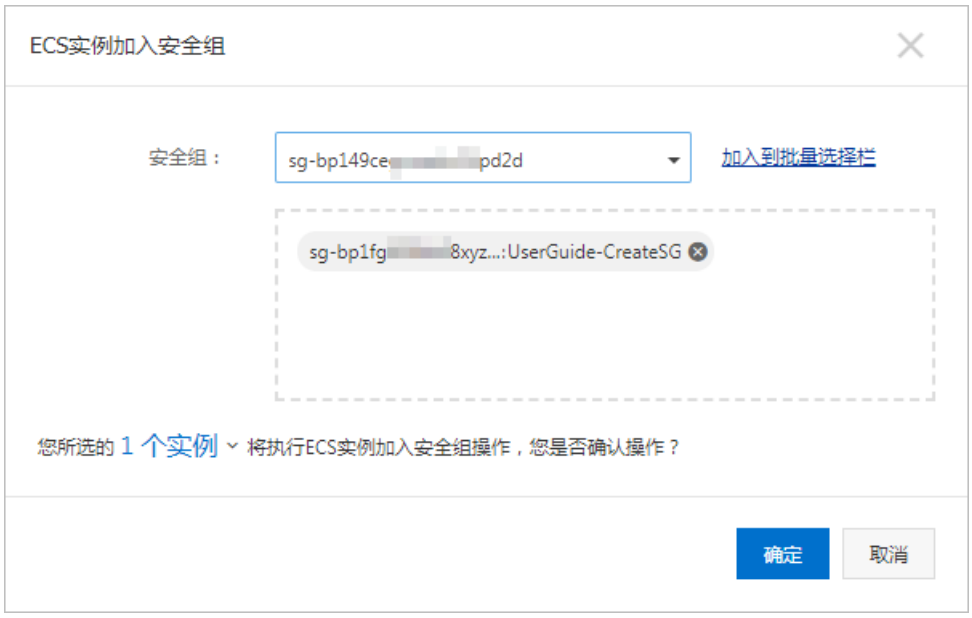
单实例加入一个或多个安全组

以下步骤指导您在实例页面将一台ECS实例加入一个或多个安全组。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**实例**页面中，找到需要加入安全组的ECS实例，您可以选择以下任意一种方式将实例加入安全组。
   - 在ECS实例详情的**安全组**页签中，将实例加入安全组。
     a. 在**操作**列中，单击**管理**。
     b. 在**实例详情**页面中，单击**安全组**页签。
     c. 单击**加入安全组**。
   - 在ECS实例列表中，将实例加入安全组。
     选择**更多 > 网路与安全组 > 加入安全组**。

5. 在**ECS实例加入安全组**对话框中，选择需要加入的安全组。

   如果您需要加入多个安全组，选择安全组后单击**加入到批量选择栏**，将会显示一个选择栏，选中的安全组自动添加到选择栏中。



6. 单击**确定**。

   加入安全组后，安全组规则对该ECS实例自动生效。

单实例或多实例加入同一个安全组

以下步骤指导您在安全组页面将一台或者多台ECS实例同时加入同一个安全组。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标安全组，在**操作**列中，单击**管理实例**。
5. 在**安全组内实例列表**页面的右上角，单击**添加实例**。
6. 在**添加实例**对话框中，选择实例ID，单击**确定**。

   如果您需要在该安全组中添加多个实例，继续单击**添加实例**，添加多个ECS实例。

   添加完成后，该安全组规则对所有的ECS实例自动生效。

后续操作

- 如果您想查看您在一个地域下创建的所有安全组，您可以查询安全组列表。具体操作，请参见查询安全组。
- 如果您不希望您的ECS实例属于某个或某几个安全组，您可以将ECS实例移出安全组。被移出的ECS实例和组内的其他ECS实例之间不再互通，建议您在操作前充分测试，确保移出ECS实例后业务可以正常运行。具体操作，请参见移出安全组。
- 如果您的业务已经不再需要一个或多个安全组，您可以删除安全组。安全组删除后，组内所有安全组规则同时被删除。具体操作，请参见删除安全组。

相关文档

- ModifyInstanceAttribute

- ModifyNetworkInterfaceAttribute

2.9. 替换ECS实例的安全组

您可以根据业务需要，将ECS实例的原安全组替换为其他安全组。

前提条件

- ECS实例和目标安全组的网络类型为专有网络VPC，且属于同一个专有网络VPC。
- 多个ECS实例批量替换安全组时，所有实例需属于同一个专有网络VPC。

背景信息

替换安全组功能适用于以下场景：

- ECS实例原安全组为普通安全组，需要替换为其他普通安全组或者企业安全组。
- ECS实例原安全组为企业安全组，需要替换为其他企业安全组或者普通安全组。

> **注意**
>
> - 安全组会影响ECS实例的网络连通，您在替换安全组前请确认已经调试好目标安全组，以免影响业务使用。
> - ECS实例不能同时加入普通安全组和企业安全组，只能加入一种类型的安全组。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**实例**页面中，您可以选择以下任意一种方式来替换ECS实例所属的安全组。
   - 在ECS实例详情的**安全组**页签中，替换安全组。
     a. 找到需要替换安全组的ECS实例，在**操作**列中，单击**管理**。
     b. 在**实例详情**页面中，单击**安全组**页签。
     c. 单击**替换安全组**。
   - 在ECS实例列表中，根据需要替换安全组的实例数量，执行不同的操作替换安全组。
     - 单个ECS实例替换安全组

       找到需要替换安全组的ECS实例，在**操作**列中，选择**更多 > 网络和安全组 > 替换安全组**。
     - 多个ECS实例批量替换安全组

       选中需要替换安全组的ECS实例，在列表底部选择**更多 > 网络和安全组 > 替换安全组**。
5. 在**实例替换安全组**对话框中，选择新安全组替换ECS实例原有的安全组。
   i. 在**安全组类型**中，选择**普通安全组**或者**企业级安全组**。

ii. 在**选择安全组**的下拉栏中选择新的安全组。

> 说明
>
> - 如果您需要选择多个安全组，单击**增加**选择其他安全组。默认情况下，一台ECS实例最多能够加入5个安全组。
> - 替换过程中，如果目标安全组选择有误，您可以在安全组列表**操作**列单击**删除**，删除后重新选择。

6. 单击**替换安全组**。

执行结果

操作完成后，ECS实例的安全组已替换成新的安全组，新安全组规则对该ECS实例自动生效。关于安全组的更多信息，请参见安全组概述。

相关文档

- ModifyInstanceAttribute

2.10. 管理安全组

2.10.1. 查询安全组

本文介绍如何在一个地域下通过不同的方式筛选安全组，以查看指定安全组的详情。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 请通过以下任一方式查询您所需要的安全组。
   - 选择**安全组名称**，在文本框中输入安全组名称并单击图标，可查询到该名称对应的安全组。
   - 选择**安全组ID**，在文本框中输入安全组ID并单击图标，可查询到该ID对应的安全组。
   - 选择**专有网络ID**，在文本框中输入专有网络ID并单击图标，可查询到该专有网络下的所有安全组。

2.10.2. 修改安全组

如果您需要修改安全组的名称、描述信息和组内连通策略，您可以修改安全组属性信息。

前提条件

您已经创建了安全组。具体操作，请参见创建安全组。

修改名称和描述信息

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。

3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，找到需要修改的安全组，单击**操作**列下的**修改**。
5. 在弹出的对话框中，修改**安全组名称**和**描述**。
6. 单击**确定**。

修改组内连通策略

加入同一个普通安全组内的实例之间默认允许所有协议、端口的互相访问，您可以根据需要修改普通安全组组内实例的连通策略。

> **说明** 企业安全组、托管安全组不支持修改组内连通策略。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，找到需要修改的安全组，单击安全组ID。
5. 在**基本信息**区域，根据需要设置**组内连通策略**。
   - **组内连通策略**是**组内互通**时，表示当前安全组内所有实例的内网默认互通。您可以单击**设置成组内隔离**，设置安全组组内内网隔离。在不添加其他访问规则的情况下，组内所有实例的内网默认不连通。
   - **组内连通策略**是**组内隔离**时，表示当前安全组内所有实例的内网默认不连通。您可以单击**设置成组内互通**，设置安全组组内内网互通。此时会忽略其他自定义访问规则，组内所有实例的内网保持默认连通。
6. 在弹出的对话框中，单击**确定**。

相关文档

- ModifySecurityGroupAttribute

2.10.3. 克隆安全组

如果您想快速创建安全组，您可以克隆安全组。支持跨地域、跨网络类型克隆安全组。

前提条件

如果您需要将安全组的网络类型更换为专有网络，您应该已经在目标地域创建了至少一个专有网络。具体操作，请参见创建和管理专有网络。

背景信息

如下场景，您可能需要克隆安全组：

- 假设您已经在地域A里创建了一个安全组SG1，此时您需要对地域B里的实例使用与SG1完全相同的规则，您可以直接将SG1克隆到地域B，而不需要在地域B从零开始创建安全组。
- 假设您已经创建了一个适用于经典网络的安全组SG2，此时您需要对一些处于VPC网络里的实例使用与SG2完全相同的规则，您可以在克隆SG2时将网络类型改为VPC，生成一个适用于VPC网络的安全组。
- 如果您需要对一个线上业务执行新的安全组规则，您可以克隆原来的安全组作为备份。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，找到需要克隆的安全组，单击**操作**列下的**克隆**。
5. 在**克隆**对话框里，设置新安全组的信息：
   - **目标地域**：选择新安全组适用的地域。目前并不支持所有的地域，支持的地域以控制台显示为准。
   - **安全组名称**：设置新安全组的名称。
   - **网络类型**：选择新安全组适用的网络类型。如果选择专有网络，您还需要在目标地域选择一个可用的专有网络。
   - **导入全部规则**：选择是否需要将原安全组所有优先级大于100的规则导入新安全组。
     - 不选中**导入全部规则**，仅克隆优先级为1~100的规则。
     - 选中**导入全部规则**，克隆优先级为1~100以及大于100的所有规则。克隆后，优先级大于100的规则将调整优先级为100。
6. 单击**确定**。

执行结果

创建成功后，**克隆**对话框会自动关闭。您可以在目标地域的**安全组**列表中看到克隆的新安全组。

2.10.4. 移出安全组

您可以根据业务需要，将ECS实例移出安全组。被移出的实例和组内的其他实例之间的网络不再互通，建议您在操作前充分测试，确保移出实例后业务可以正常运行。

前提条件

ECS实例已加入两个或两个以上安全组。

背景信息

您可以按需选择以下一种方式，将实例移出安全组。

- 如果您需要将某一特定实例移出所属的安全组，操作步骤请参见移出特定实例。
- 如果您需要将多个实例移出某一安全组，操作步骤请参见移出多个实例。

移出特定实例

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**实例列表**页面中，找到需要移出安全组的实例，单击**操作**列下的**管理**。
5. 在**实例详情**页面中，单击**安全组**页签。
6. 找到需要移出的安全组，单击**操作**列下的**移出**。
7. 单击**确定**。

移出多个实例

1. 登录ECS管理控制台。

2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组列表**页面中，找到需要移出实例的安全组，单击安全组ID。
5. 在左侧导航栏中，单击**安全组内实例列表**。
6. 勾选一个或多个实例，单击**移出安全组**。
7. 单击**确定**。

相关文档

- ModifyInstanceAttribute
- ModifyNetworkInterfaceAttribute

2.10.5. 编辑安全组标签

标签用于标识具有相同特征的资源，例如所属组织相同或用途相同的安全组，您可以基于标签方便地检索和管理资源。本文介绍如何编辑已有安全组的标签。

背景信息

标签的使用说明、支持资源、使用限制等信息，请参见标签概述和标签使用限制。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标安全组，在**标签**列将鼠标悬浮至图标，然后单击**编辑标签**。
5. 在**编辑标签**对话框，选择已有标签或新建标签，然后单击**确定**。

后续步骤

绑定标签后，您可以基于标签筛选安全组并完成各种管理动作，例如将ECS实例加入一类安全组、为一类安全组添加安全组规则等。

2.10.6. 删除安全组

如果您的业务已经不再需要一个或多个安全组，您可以删除安全组。安全组删除后，组内所有安全组规则同时被删除。

前提条件

- 待删除的安全组内不存在ECS实例。如果安全组内有ECS实例，您需要将实例移出安全组。具体操作，请参见移出安全组。
- 待删除的安全组与其他安全组之间没有授权行为。如果该安全组被其他安全组授权，您可以根据页面提示，删除相应的授权规则。具体操作，请参见删除安全组规则。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，选中一个或多个安全组，在页面底部单击**删除**。
5. 在**删除安全组**对话框中，确认信息后，单击**确定**。

相关文档

- DeleteSecurityGroup

2.11. 管理安全组规则

2.11.1. 安全组规则概述

安全组规则是您自定义的访问规则，用于控制安全组内实例的入方向访问和出方向访问。

安全组规则属性

在添加或修改一条安全组规则时，需要设置的属性如下表所示。

属性	说明
规则方向	网络类型影响规则方向的分类： • 如果安全组网络类型为专有网络，安全组规则分为入方向、出方向，一条安全组规则同时适用于控制公网和内网访问。 • 如果安全组网络类型为经典网络，安全组规则分为公网入方向、公网出方向、入方向（即内网入方向）、出方向（即内网出方向），您需要为控制公网和内网访问分别创建安全组规则。 规则方向影响匹配要素： • 入方向访问：访问请求和安全组规则的传输层协议、目的端口、源IP地址都相同时视为匹配成功。 • 出方向访问：访问请求和安全组规则的传输层协议、目的端口、目的IP地址都相同时视为匹配成功。 **说明** 在控制台创建的安全组规则默认为三元组规则。如果您需要更精确地控制访问，可以通过OpenAPI创建五元组规则，基于源IP地址、源端口、目的IP地址、目的端口及传输层协议控制访问。更多信息，请参见安全组五元组规则。

属性	说明
授权策略	支持允许和拒绝策略。如果两条安全组规则只有授权策略不同，则拒绝策略的安全组规则生效。
优先级	优先级的取值范围为1~100，数值越小，代表优先级越高。
协议类型	传输层协议的类型，支持TCP、UDP、ICMP(IPv4)、ICMP(IPv6)和GRE。
端口范围	入方向访问和出方向访问的目的端口，可以设置一个或多个。关于典型应用的默认端口，请参见典型应用的常用端口。
授权对象	支持针对以下对象授权： • 单一IP地址：例如 `192.168.0.100` 、 `2408:4321:180:1701:94c7:bc38:3bfa:` 。 • CIDR地址块：例如 `192.168.0.0/24` 、 `2408:4321:180:1701:94c7:bc38:3bfa:***/128` 。 • 其他安全组：授权其他安全组内的实例访问本安全组内的实例，实现内网互通。支持授权当前账号或其他账号下的安全组。 说明 仅普通安全组支持针对其他安全组授权。 • 前缀列表：前缀列表是一些网络前缀（即CIDR地址块）的集合，授权对象为前缀列表时，这条安全组规则适用于前缀列表中的所有CIDR地址块，例如 `192.168.0.0/24,172.16.0.0/16` 。

安全组规则过滤访问请求流程

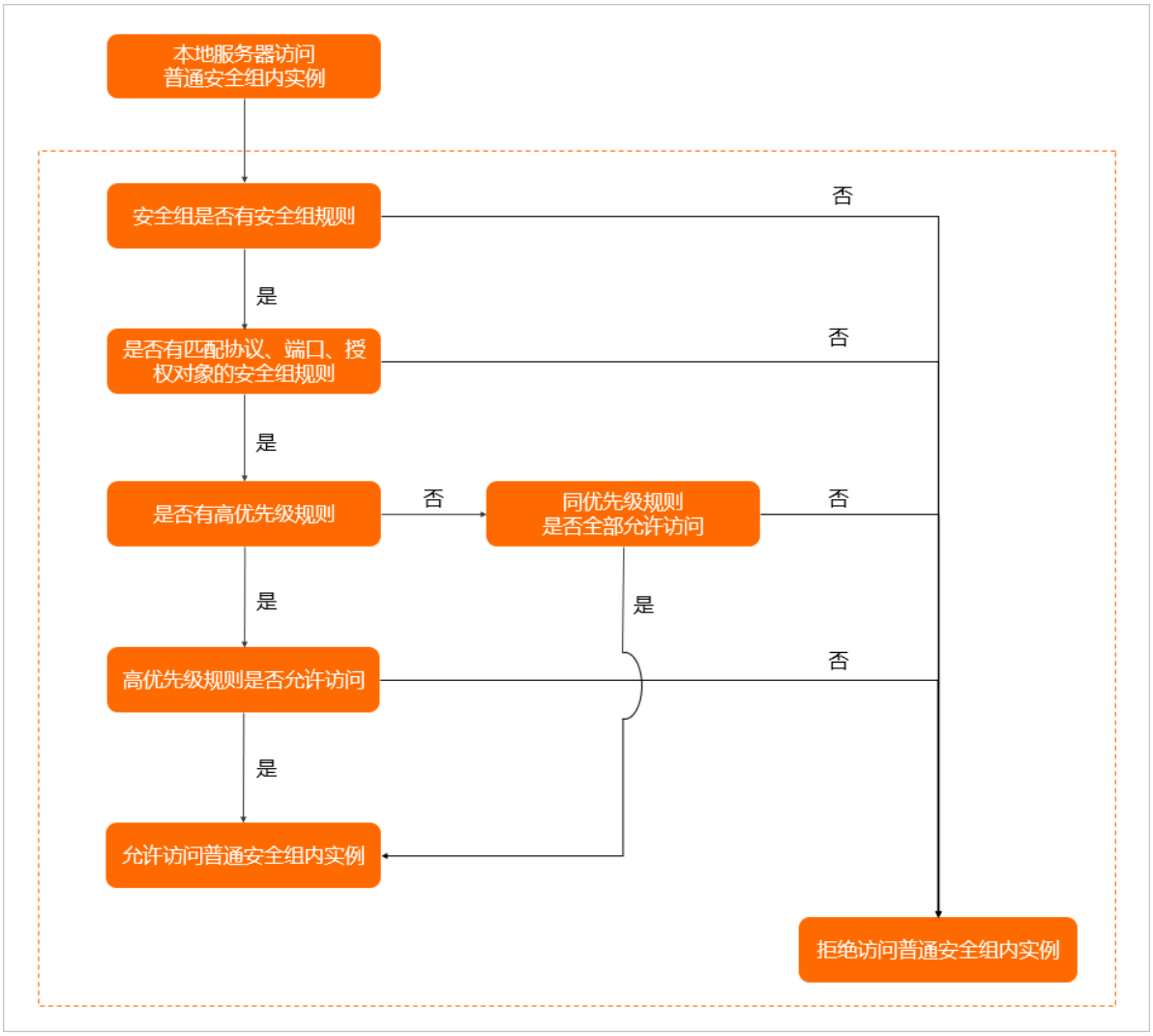
如果一台实例加入了多个安全组，则所有安全组的安全组规则均应用于该实例。检测到访问请求时，系统会逐一尝试匹配安全组规则。如果基于协议、端口、授权对象匹配到了多条安全组规则，则继续通过优先级和授权策略来判定最终生效的安全组规则，最终结果为允许访问时才建立会话。

如果访问出现异常，您可以按需添加或修改安全组规则，新的安全组规则会自动应用于安全组内所有实例。

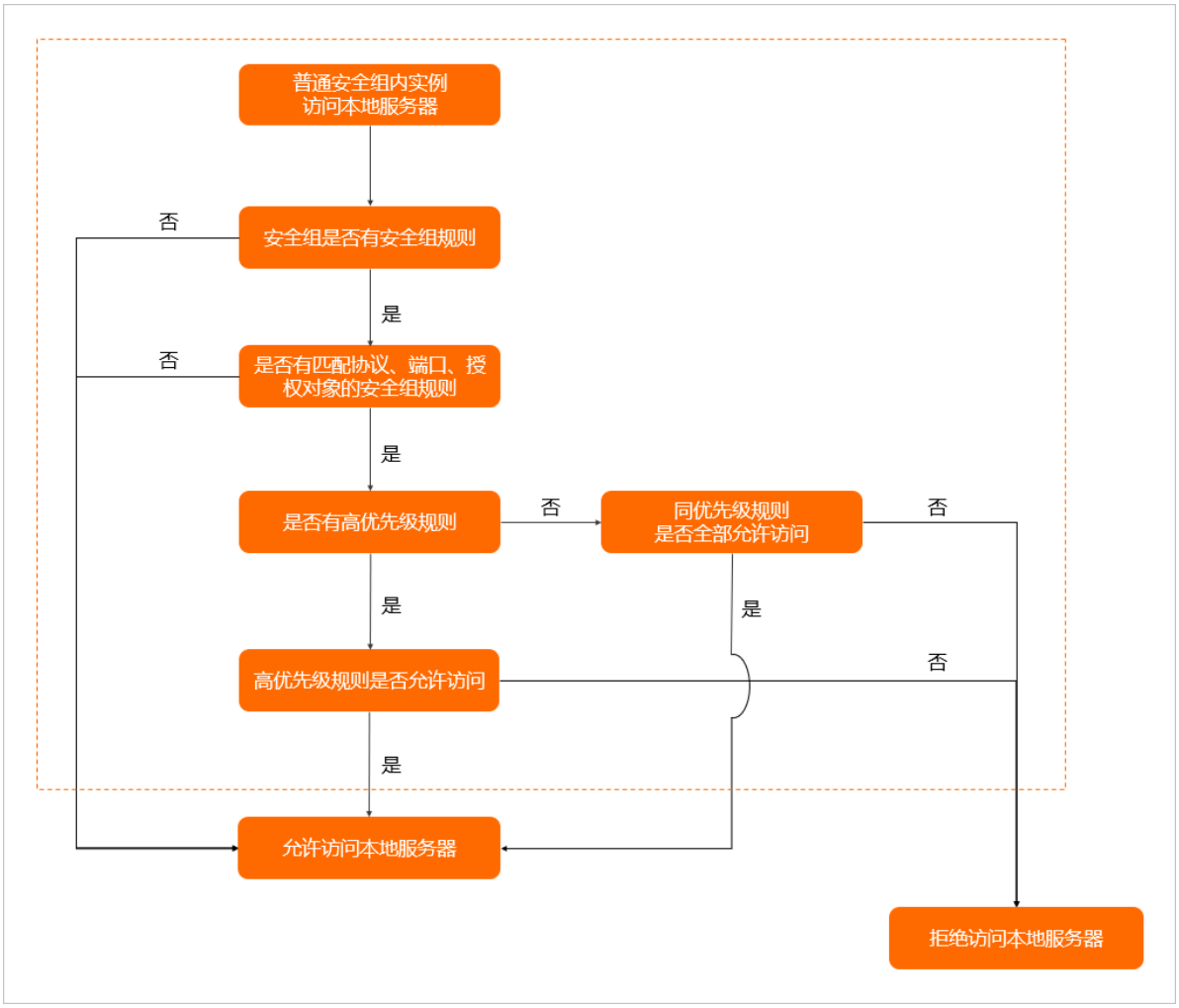
本文以本地服务器和普通安全组内的实例之间互相访问为例，通过流程图介绍基于安全组规则过滤访问请求的流程。下方流程图中，安全组中没有安全组规则代表您已删除安全组内所有的安全组规则，包括系统自动添加的默认规则。

说明 在控制台创建安全组时，系统会自动添加默认规则。更多默认规则的信息，请参见默认安全组和安全组和安全组规则。

- 本地服务器访问普通安全组内的实例（入方向），流程如下图所示。



- 普通安全组内的实例访问本地服务器（出方向），流程如下图所示。



安全组规则示例

如果您需要使用SSH密钥对远程连接Linux实例，以在专有网络安全组中添加安全组规则为例，如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
入方向	允许	1	自定义TCP	目的：22/22	源：0.0.0.0/0

> **说明** `0.0.0.0/0` 为允许所有IP远程连接实例。为安全起见，建议您在实际业务中将授权对象设置为特定的IP访问，遵循最小授权原则。

在未添加安全组规则时，普通安全组允许出方向访问。如果您希望将安全组作为白名单使用，可以设置默认拒绝所有出方向访问。以在专有网络安全组中添加安全组规则为例，如下表所示。

规则方向	授权策略	优先级	协议类型	端口范围	授权对象
出方向	拒绝	100	全部	目的：-1/-1	目的：0.0.0.0/0

更多安全组规则示例，请参见安全组应用案例ECS安全组配置操作指南。

2.11.2. 查询安全组规则

添加安全组规则后，您可以在控制台上查询安全组规则的详细信息。

前提条件

请确认您已创建了安全组，并且已在安全组中添加了安全组规则。具体操作，请参见创建安全组和添加安全组规则。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到需要查询规则的安全组，单击**操作**列下的**配置规则**。
5. 单击安全组规则所属的方向，可以查询到各自分类的安全组规则。
   - 如果您需要查询专有网络类型的安全组规则，请选择**入方向**或**出方向**。
   - 如果您需要查询经典网络类型的安全组规则，请选择**内网入方向**、**内网出方向**、**公网入方向**或**公网出方向**。

相关文档

- DescribeSecurityGroupAttribute

2.11.3. 修改安全组规则

安全组规则设置不当会造成严重的安全隐患。您可以修改安全组中不合理的安全组规则，保证ECS实例的网络安全。

前提条件

请确认您已创建了安全组，并且已在安全组中添加了安全组规则。具体操作，请参见创建安全组和添加安全组规则。

背景信息

如果安全组规则对特定端口的访问不做限制，会造成严重的安全隐患。您可以通过修改安全组规则保证ECS实例的网络安全。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到需要修改安全组规则的安全组，单击**操作**列下的**配置规则**。
5. 单击安全组规则所属的方向。
   - 如果您需要修改专有网络类型的安全组规则，请选择**入方向**或**出方向**。
   - 如果您需要修改经典网络类型的安全组规则，请选择**内网入方向**、**内网出方向**、**公网入方向**或**公网出方向**。

6. 找到需要修改的安全组规则，单击**操作**列下的**编辑**。
   - 如何配置安全组规则，请参见添加安全组规则。
   - 安全组规则的应用案例，请参见安全组规则的典型应用。
7. 根据需要修改完安全组规则后，单击**保存**。

2.11.4. 还原安全组规则

如果您需要对一个线上业务执行新的安全组规则，您可以先克隆原来的安全组作为备份，再修改安全组规则。如果新的安全组规则对线上业务产生了不利影响，您可以全部或部分还原安全组规则。

前提条件

- 原安全组与目标安全组必须在同一个地域。
- 原安全组与目标安全组必须为同一种网络类型。

背景信息

还原安全组规则是指将一个原安全组里的规则全部或部分地还原为目标安全组规则的过程。

- **全部还原**：还原时，系统在原安全组中删除目标安全组中没有的规则，并在原安全组中添加只有目标安全组中才有的规则。还原操作后，原安全组里的规则与目标安全组里的规则完全相同。
- **部分还原**：仅将目标安全组中才有的规则添加到原安全组里，忽略原安全组中有而目标安全组中没有的规则。

> **说明**
>
> 还原安全组规则有以下限制： 目标安全组中如果有系统级的安全组规则（优先级为110），还原时无法创建该类规则，还原后，原安全组中的规则可能会与预期不同。如果您需要这些安全组规则，请手动创建相似规则（优先级可以设为100）。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组列表**页面中，找到需要还原安全组规则的安全组，单击**操作**列下的**还原规则**。
5. 在**还原规则**对话框里，完成以下配置。
   i. 选择**目标安全组**，目标安全组必须与原安全组拥有不一样的规则。
   ii. 选择**还原策略**。
      - 如果您需要原安全组与目标安全组拥有完全一致的规则，请选择**全部还原**。
      - 如果您只需要在原安全组中添加只有目标安全组中才有的规则，请选择**部分还原**。

iii. 预览还原结果。

- 绿色显示的是只有目标安全组中才有的规则。无论是**全部还原**还是**部分还原**，这部分规则都会被添加到原安全组中。
- 红色显示的是目标安全组中没有的规则。
  - 如果选择**全部还原**，系统会在原安全组中删除这部分规则。
  - 如果选择**部分还原**，原安全组中这部分规则仍会保留。

iv. 确认无误后，单击**确定**。
创建成功后，**还原规则**对话框会自动关闭。

执行结果

在**安全组列表**中，找到刚完成还原操作的原安全组，在**操作**列中，单击**配置规则**进入**安全组规则**页面，查看更新后的安全组规则。

2.11.5. 导出安全组规则

安全组规则支持导出功能，您可以将安全组下的安全组规则导出为JSON文件或CSV文件，用于本地备份。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，找到需要导出安全组规则的安全组，单击**操作**列下的**配置规则**。
5. 在**访问规则**区域，单击**导出**，并单击保存的文件格式，下载并保存到本地。
   - **JSON格式**

     JSON文件命名规则示例为：*ecs_${region_id}_${groupID}.json*

     假设regionID是*cn-qingdao*，groupID是*sg-123*，导出的JSON文件名称则是*ecs_cn-qingdao_sg-123.json*。
   - **CSV格式**

     CSV文件命名规则示例为：*ecs_sgRule_${groupID}_${region_id}_${time}.csv*

     假设regionID是*cn-qingdao*，groupID是*sg-123*，time是*2020-01-20*，导出的CSV文件名称则是*ecs_sgRule_sg-123_cn-qingdao_2020-01-20.csv*。

2.11.6. 导入安全组规则

安全组规则支持导入功能。您可以将导出的安全组规则文件导入到安全组中，快速创建或恢复安全组规则。

背景信息

安全组支持导入不同地域的安全组规则。

您可以单击**导出**，导出JSON或CSV格式的安全组规则文件作为模板。如果需要自定义安全组规则，请按照格式修改文件内容。

操作步骤

1. 登录ECS管理控制台。

2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，找到需要导入安全组规则的安全组，在**操作**列单击**配置规则**。
5. 在**访问规则**区域，单击**导入安全组规则**。
6. 在**导入安全组规则**对话框中，单击**选择文件**，选择本地的JSON或CSV文件。

   对话框中将会自动生成预览规则，显示以下信息：
   - 检查结果。如果存在导入失败的规则，您可以将光标移到警告图标上查看失败原因。
   - 导入规则详情。

   > **说明** 导入的安全组规则不能超过200条，超出限制的规则会导入失败。导入的新规则不会覆盖原有规则。

7. 单击**开始导入**。

2.11.7. 删除安全组规则

如果您不再需要通过某条安全组规则允许或禁止访问安全组内实例，可以删除安全组规则。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**安全组**页面中，找到需要删除规则的安全组，单击**操作**列下的**配置规则**。
5. 根据安全组的网络类型选择页签。
   - 如果为专有网络，请选择**入方向**或**出方向**。
   - 如果为经典网络，请选择**入方向**、**出方向**、**公网入方向**或**公网出方向**。
6. 找到需要删除的安全组规则，单击**操作**列下的**删除**。
7. 在弹出的对话框中阅读提示信息，确认无误后，单击**确定**。

相关文档

- RevokeSecurityGroup
- RevokeSecurityGroupEgress

3.SSH密钥对

3.1. SSH密钥对概述

阿里云SSH密钥对是一种安全便捷的登录认证方式，由公钥和私钥组成，仅支持Linux实例。

SSH密钥对介绍

SSH密钥对通过加密算法生成一对密钥，默认采用RSA 2048位的加密方式。要使用SSH密钥对登录Linux实例，您必须先创建一个密钥对，并在创建实例时指定密钥对或者创建实例后绑定密钥对，然后使用私钥连接实例。

成功创建SSH密钥对后：

- 阿里云会保存SSH密钥对的公钥部分。在Linux实例中，公钥内容放在*~/.ssh/authorized_keys*文件内。
- 您需要下载并妥善保管私钥。私钥使用未加密的PEM（Privacy-Enhanced Mail）编码的 `PKCS#8` 格式。

功能优势

相较于用户名和密码认证方式，SSH密钥对有以下优势：

- 安全性：SSH密钥对登录认证更为安全可靠。
  - 密钥对安全强度远高于常规用户口令，可以杜绝暴力破解威胁。
  - 不可能通过公钥推导出私钥。
- 便捷性：
  - 如果您将公钥配置在Linux实例中，那么，在本地或者另外一台实例中，您可以使用私钥通过SSH命令或相关工具登录目标实例，而不需要输入密码。
  - 便于远程登录大量Linux实例，方便管理。如果您需要批量维护多台Linux实例，推荐使用这种方式登录。

使用限制

使用SSH密钥对有如下限制：

- 如果使用SSH密钥对登录Linux实例，将会禁用密码登录，以提高安全性。
- 仅支持Linux实例。
- 目前，ECS只支持创建2048位的RSA密钥对。
- 一个云账号在一个地域最多可以拥有500个密钥对。
- 通过控制台绑定密钥对时，一台Linux实例只能绑定一个密钥对，如果您的实例已绑定密钥对，绑定新的密钥对会替换原来的密钥对。 如果您有使用多个密钥对登录实例的需求，可以在实例内部手动修改*~/.ssh/authorized_keys*文件，添加多个密钥对。
- 已停售的实例规格无法使用SSH密钥对。详情请参见已停售的实例规格。
- 基于数据安全考虑，在实例状态为**运行中**（ `Running` ）时绑定或者解绑密钥对，您需要重启实例使操作生效。

生成方式

SSH密钥对的生成方式包括：

- 由ECS生成，默认采用RSA 2048位的加密方式。具体操作，请参见创建SSH密钥对。

> 注意 如果您的密钥对由ECS生成，那么在首次生成密钥对时，请务必下载并妥善保存私钥。当该密钥对绑定某台实例时，如果没有私钥，您将无法登录实例。

- 由您采用SSH密钥对生成器生成后再导入ECS，导入的密钥对必须支持以下任一种加密方式：
  - rsa
  - dsa
  - ssh-rsa
  - ssh-dss
  - ecdsa
  - ssh-rsa-cert-v00@openssh.com
  - ssh-dss-cert-v00@openssh.com
  - ssh-rsa-cert-v01@openssh.com
  - ssh-dss-cert-v01@openssh.com
  - ecdsa-sha2-nistp256-cert-v01@openssh.com
  - ecdsa-sha2-nistp384-cert-v01@openssh.com
  - ecdsa-sha2-nistp521-cert-v01@openssh.com

3.2. 管理SSH密钥对

3.2.1. 创建SSH密钥对

创建密钥对后，系统将自动下载私钥，请您妥善保管。使用密钥对绑定ECS实例后，如果没有私钥，您将无法登录该ECS实例。您在一个地域最多可以拥有500个密钥对。本文介绍如何在ECS控制台上创建SSH密钥对。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 密钥对**。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击**创建密钥对**。
5. 在**创建密钥对**页面，完成以下配置。

配置项	描述
密钥对名称	密钥对名称不能和已有密钥对重复。长度为2~128个字符，不能以特殊字符及数字开头，只可包含特殊字符中的英文句号（.）、下划线（_）、短划线（-）和冒号（:）。
创建类型	您可以选择以下任一类型创建密钥对。建议您选择**自动新建密钥对**，并及时保存私钥。 ○ **自动新建密钥对**：系统会为您自动创建密钥对。创建完成后将自动下载私钥，您只有这一次下载私钥的机会，因此请妥善保存私钥文件。 ○ **导入已有密钥对**：您可以自行导入Base64编码的公钥内容。

配置项	描述
资源组	您可以为密钥对指定一个资源组，实现对资源的分组管理，详情请参见资源组。
标签	您可以为密钥对绑定一个或多个标签，便于搜索和资源聚合，详情请参见标签概述。

6. 单击**确定**。

执行结果

创建成功后，浏览器自动下载私钥文件（*密钥对名称.pem*）到本地电脑。

> **注意** 私钥文件只在创建密钥对时自动下载到本地，ECS控制台不会保存私钥文件。如果私钥文件丢失将无法找回，请您妥善保存。

后续步骤

创建密钥对后，您需要继续为ECS实例绑定密钥对，然后可以通过密钥对登录ECS实例。

- 绑定密钥对的具体操作，请参见绑定SSH密钥对。
- 通过密钥对登录ECS实例的具体操作，请参见通过密钥认证登录Linux实例。

相关文档

- CreateKeyPair

3.2.2. 导入SSH密钥对

除在ECS管理控制台新建密钥对外，如果您已经持有使用第三方工具生成的SSH密钥对，可以将公钥导入阿里云，生成新的密钥对。

前提条件

已获取待导入密钥对的公钥信息。若尚未获取，请参见查看公钥信息。

背景信息

> **说明**
> - 不要导入私钥。请您妥善保存私钥。使用密钥对绑定ECS实例后，如果没有私钥，您将无法登录该ECS实例。
> - 一台ECS实例只能导入一个公钥。

一个账号在一个地域最多可以拥有500个密钥对。更多详情，请参见SSH密钥对使用限制。

导入阿里云的公钥必须使用 `Base64` 编码，且必须支持下列加密方式中的一种：

- rsa
- dsa
- ssh-rsa
- ssh-dss

- ecdsa
- ssh-rsa-cert-v00@openssh.com
- ssh-dss-cert-v00@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ssh-dss-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 密钥对**。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击**创建密钥对**。
5. 设置密钥对名称，并选择**导入已有密钥对**。

   > **说明** 密钥对名称不能重复。否则，控制台会提示密钥对已存在。

6. 在**公钥内容**文本框中，输入要导入的公钥。
7. 单击**确定**。

后续步骤

绑定SSH密钥对

相关文档

- ImportKeyPair

3.2.3. 绑定SSH密钥对

您可以在创建实例时指定SSH密钥对，也可以在创建实例后绑定SSH密钥对。本文介绍如何在创建实例后绑定SSH密钥对。如果ECS实例原先使用密码认证，绑定密钥对后，密码验证方式自动失效。

背景信息

在控制台操作时，一台ECS实例只能绑定一个SSH密钥对。如果ECS实例已经绑定了SSH密钥对，绑定新密钥对后，新密钥自动替换原有的密钥。

> **说明** 在Linux实例中，公钥信息保存在*~/.ssh/authorized_keys*文件内。通过修改公钥文件，您可以添加多个密钥对或替换现有的密钥对，具体请参见添加或替换密钥对。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 密钥对**。
3. 在顶部菜单栏左上角处，选择地域。

4. 找到需要操作的密钥对，在**操作**列中，单击**绑定密钥对**。
5. 在**选择ECS实例**栏中，选中需要绑定该密钥对的ECS实例名称，单击>图标，移入**已选择**栏中。

   如果**选择ECS实例**栏中的ECS实例名称显示为灰色，表示该实例为Windows实例，不支持SSH密钥对。
6. 单击**确定**。
7. 如果ECS实例处于**运行中**（*Running*）状态，重启实例使操作生效：
   i. 在左侧导航栏，单击**实例与镜像 > 实例**。
   ii. 找到需要操作的实例，在**操作**列中，选择**更多 > 实例状态 > 重启**。
   iii. 在**重启实例**弹窗中，单击**确定**。

后续步骤

- ECS实例绑定SSH密钥对后，您就可以通过SSH密钥对登录ECS实例。具体操作，请参见通过密钥认证登录Linux实例。
- 如果您在绑定密钥对之后想使用密码方式登录实例，可以通过重置实例密码实现。如果在绑定密钥对之后重置了实例密码，使用密钥对方式和使用密码方式均能登录实例。重置实例密码请参见重置实例密码。

相关文档

- AttachKeyPair

3.2.4. 解绑SSH密钥对

本文介绍如何在ECS控制台上解绑SSH密钥对。

前提条件

SSH密钥对已绑定了ECS实例。具体操作，请参见绑定SSH密钥对。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 密钥对**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到需要操作的密钥对，在**操作**列中，单击**解绑密钥对**。
5. 在**选择ECS实例**栏中，选中需要解绑的ECS实例名称，单击>图标，移入**已选择**栏中。
6. 单击**确定**。
7. 如果ECS实例处于**运行中**状态，重启实例使操作生效。
   i. 在左侧导航栏，单击**实例与镜像 > 实例**。
   ii. 找到需要操作的实例，在**操作**列中，选择**更多 > 实例状态 > 重启**。
   iii. 在**重启实例**弹窗中，单击**确定**。

后续步骤

解绑密钥对之后，必须重置实例密码才能继续使用root密码方式登录实例。具体操作，请参见重置实例密码。

> **说明** 如果在解绑密钥对之前已经重置了实例密码，则解绑密钥对之后，可以直接使用密码方式登录，无需再次重置实例密码。

相关文档

- DetachKeyPair

3.2.5. 删除SSH密钥对

删除SSH密钥对后不可恢复，但是正在使用该密钥对的实例不受影响，实例信息中仍然会显示被删除的密钥对名称。

前提条件

请确保您已创建了SSH密钥对。具体操作，请参见创建SSH密钥对。

背景信息

在删除SSH密钥对之前，您需要了解以下信息：

- 如果您的密钥对已经绑定实例，而且在删除前未解绑实例，删除后，您将不能再用相同的名称创建密钥对。否则，创建或导入密钥对时，输入这个名称，控制台会报错密钥对已存在。
- 如果您的密钥对在删除前未绑定实例或者已经解绑实例，删除后，您仍可以使用相同的名称创建密钥对。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**网络与安全 > 密钥对**。
3. 在顶部菜单栏左上角处，选择地域。
4. 选中一个或多个需要删除的密钥对。
5. 单击**删除**。

相关文档

- DeleteKeyPairs

3.2.6. 查看公钥信息

如果您想设置一组ECS使用相同的公钥文件，而本地又没有公钥文件的备份，您可以通过以下三种方式查看并获取公钥信息。

本地为Windows操作系统

完成以下操作，查看公钥信息：

1. 启动PuTTYgen。
2. 单击**Load**。
3. 选择*.ppk*或*.pem*文件。
   PuTTYgen会显示公钥信息。

本地为Linux或Mac系统

运行**ssh-keygen**命令，并指定*.pem*文件的路径。

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

返回公钥信息，类似如下所示：

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABA****+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHex21hl1au77Gkm
nIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIPxxxxxxxxxx/fctNuKjcmMMOA8YUT+sJKn3l7rCLkesE+S5880yNdRjBii
Uy40kyr7Y+fqGVdSOHGMXZQPpkBtojcxxxxxxxxxxx/htEqGa/Jq4fH7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKuIHdM
WOPvjxxxxxxxxx+lHtTGiAIRG1riyNRVC47ZEVCxxxxxx
```

说明 如果该命令失败，请运行 `chmod 400 my-key-pair.pem` 命令更改权限，确保只有您才能查看该文件。

在实例内部查看公钥信息

公钥内容放在*~/.ssh/authorized_keys*文件内。在实例内打开该文件，则返回公钥信息。

3.2.7. 添加或替换密钥对

在Linux实例内部，您可以添加多个密钥对，允许多个密钥对访问该实例。您也可以替换现有的密钥对。

前提条件

请确保您已获取新密钥对的公钥信息。详细步骤请参见查看公钥信息。

背景信息

在Linux实例中，公钥信息保存在*~/.ssh/authorized_keys*文件内。通过修改公钥文件，您可以添加多个密钥对或替换现有的密钥对。

说明 在控制台操作时，实例仅支持绑定一个密钥对。如果您仅需要一个密钥对，建议您直接通过控制台进行绑定，详细步骤请参见绑定SSH密钥对。

操作步骤

1. 使用现有的密钥对连接ECS实例。
2. 运行**vim .ssh/authorized_keys**命令打开文件。
3. 添加或者替换公钥信息。
   - 添加公钥信息：在现有的公钥信息下方添加新的公钥信息，并保存。

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCys3aOkFm1Xh8iN0lijeQF5mz9Iw/FV/bUUduZjauiJa1KQ
JSF4+czKtqMAv38QEspiWStkSfpTn1g9qeUhfxxxxxxxxxx+XjPsf22fRem+v7MHMa7KnZWiHJxO62D4Ihvv2
hKfskz8K44xxxxxxxxx+u17IaL2l2ri8q9YdvVHt0Mw5TpCkERWGoBPE1Y8vxFb97TaE5+zc+2+eff6xxxxx
xxxxx/feMeCxpx6Lhc2NEpHIPxMpjOv1IytKiDfWcezA2xxxxxxxxxx/YudCmJ8HTCnLId5LpirbNE4X08Bk7
tXZAxxxxxxxxxx/FKB1Cxw1TbGMTfWxxxxxxxxxx imported-openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHex
21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIPxxxxxxxxxxx/fctNuKjcmMMOA8YUT+sJKn3l7rC
LkesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcxxxxxxxxxx/htEqGa/Jq4fH7bR6CYQ2XgH/
hCap29Mdi/G5Tx1nbUKuIHdMWOPvjxxxxxxxxxx+lHtTGiAIRG1riyNRVC47ZEVCg9iTWWGrWFvxxxxxxxxxxx
/9H9mPCO1Xt2fxxxxxxxxBtmR imported-openssh-key
```

> **说明** 如果公钥文件中有多个公钥信息，则使用其对应的多个私钥均能登录实例。

- 替换公钥信息：删除现有的公钥信息，添加新的公钥信息，并保存。

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6vYrExwT4WU4fsaRcVXGV2Mg9RHex
21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIP6t0Mk5aPkK/fctNuKjcmMMOA8YUT+sJKn3l7rCL
kesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcV14uAy0yV6/htEqGa/Jq4fH7bR6CYQ2XgH/h
Cap29Mdi/G5Tx1nbUKuIHdMWOPvjGACGcXclex+lHtTGiAIRG1riyNRVC47ZEVCg9iTWWGrWFvVlnI0E3Deb/
9H9mPCO1Xt2fxxxxxxxxBtmR imported-openssh-key
```

如果使用新的私钥能够登录ECS实例，表示添加或者替换密钥对成功。

4.管理身份和权限

4.1. 访问控制RAM介绍

访问控制RAM用于为人员、云服务等指定身份并基于身份授予资源访问权限，从而控制对阿里云资源的访问。

身份管理

访问控制RAM中的身份包括实体身份（RAM用户、RAM用户组）和虚拟身份（RAM角色）。

- RAM用户有确定的登录密码和访问密钥，RAM用户组则用于分类职责相同的RAM用户，RAM用户和RAM用户组均可以被赋予一组权限策略。RAM用户可以对应企业内的人员、应用等，在需要协同使用资源的场景中，避免直接共享阿里云账号的密码等机密信息，缩小机密信息的可见范围，并为RAM用户和RAM用户组赋予最小权限，即使不慎泄露机密信息，也不会危及阿里云账号下的所有资源。
- RAM角色有确定的身份，可以被赋予一组权限策略，但是没有确定的登录密码或访问密钥。RAM角色需要由一个受信的实体扮演，该实体在扮演RAM角色时即获得RAM角色的权限。在云产品通信的场景中，为受信的实体（例如ECS实例）绑定RAM角色后，该实体可以基于STS（Security Token Service）临时凭证访问其他云产品的API，避免将AccessKey写在配置文件中等高危操作，保证AccessKey的安全。

权限管理

访问控制RAM通过权限策略描述授权的具体内容，权限策略包括固定的基本元素，更多信息，请参见权限策略基本元素。为RAM用户、RAM用户组、RAM角色添加一组权限策略后，即可让其有权限访问指定资源。

权限策略分为系统策略和自定义策略。

- 系统策略：阿里云预定义的常用权限策略，您只能使用不能修改。部分云服务器ECS相关的系统策略如下：
  - AliyunECSFullAccess：云服务器ECS的管理权限，包括创建、查看、删除相关资源等操作。
  - AliyunECSReadOnlyAccess：云服务器ECS的只读权限，只可查看相关资源。
  - AliyunECSNetworkInterfaceManagementAccess：弹性网卡的管理权限，包括创建、查看、删除弹性网卡等操作。
  - AliyunECSAssistantFullAccess：云助手命令的管理权限，包括创建、执行、查看、删除云助手命令等操作。
  - AliyunECSAssistantReadonlyAccess：云助手命令的只读权限，只可查看云助手命令相关信息。
  - AliyunECSImageExportRolePolicy：导出ECS实例镜像所需的权限，包括读OSS Bukcet、读写OSS Object等操作。
  - AliyunECSImageImportRolePolicy：导入镜像所需的权限，包括读OSS Bukcet、读OSS Object操作。
  - AliyunECSInstanceForYundunSysTrustRolePolicy：安全增强型实例使用阿里云可信服务所需的权限。
  - AliyunECSDiskEncryptRolePolicy：加密云盘所需的权限。

  更多系统策略的详情信息，请参见系统策略示例。
- 自定义策略：您按需自行创建和维护的权限策略，关于自定义策略的操作和示例，请参见创建自定义权限策略和权限策略示例库概览。

应用示例

在企业内部控制员工的资源使用权限：

1. 为需要创建和管理资源的职位创建SysAdmins用户组，并添加权限策略，授予执行所有操作的权限。

2. 为需要使用资源的职位创建Developers用户组，并添加权限策略，授予调用StartInstance、StopInstance、DescribeInstances接口的权限。
3. 为员工创建RAM用户，并按照各自职位加入用户组。
4. 为加强网络安全控制，添加权限策略，规定如果组内用户的IP地址不是来自企业网络，则拒绝其访问资源。
5. 如果某开发人员的职位变更为系统管理员，将其RAM用户从Developers用户组移动到SysAdmins用户组。
6. 如果Developers用户组的RAM用户需要更大权限，修改用户组的权限策略即可应用到用户组中的所有RAM用户。

为ECS实例绑定RAM角色，然后基于STS临时凭证访问其他阿里云产品：

- AliyunECSImageExportDefaultRole：为ECS实例绑定该角色后，即可获得导出ECS实例镜像所需的权限，对应的默认权限策略为AliyunECSImageExportRolePolicy。
- AliyunECSImageImportDefaultRole：为ECS实例绑定该角色后，即可获得导入镜像所需的权限，对应的默认权限策略为AliyunECSImageImportRolePolicy。
- AliyunECSInstanceForYundunSysTrustRole：为ECS实例绑定该角色后，即可获得使用阿里云可信服务所需的权限，对应的默认权限策略为AliyunECSInstanceForYundunSysTrustRolePolicy。
- AliyunECSDiskEncryptDefaultRole：为ECS实例绑定该角色后，即可获得加密云盘所需的权限，对应的默认权限策略为AliyunECSDiskEncryptRolePolicy。

相关文档

- 什么是访问控制

4.2. 通过RAM用户控制资源访问

在协同使用资源的场景下，根据实际的职责权限情况，您可以创建多个RAM用户并为其授予不同的权限，实现不同RAM用户可以分权管理不同的资源，从而提高管理效率，降低信息泄露风险。本文介绍如何创建RAM用户并授予特定权限策略，从而控制对云服务器ECS资源的访问。

操作步骤

1. 创建RAM用户。

   具体操作，请参见创建RAM用户。

2. （可选）创建自定义策略。

   阿里云提供了访问云服务器ECS资源的系统策略，更多信息，请参见系统策略示例。如果系统策略不能满足需求，您还可以创建自定义策略，具体操作，请参见创建自定义权限策略。

   创建自定义策略时，如果配置模式选择**脚本配置**，Statement结构下的Action和Resource参数取值说明，请参见鉴权列表。更多参数取值说明，请参见权限策略语法和结构。

   - 脚本配置策略示例一：允许RAM用户创建按量付费实例。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                    "ecs:DescribeImages",
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeKeyPairs",
                "ecs:DescribeTags",
                "ecs:RunInstances"
          ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

- 脚本配置策略示例二：允许RAM用户创建包年包月实例。其中bss相关API主要用于查看并支付包年包月订单，其对应的系统策略为 `AliyunBSSOrderAccess` 。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                    "ecs:DescribeImages",
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeKeyPairs",
                "ecs:DescribeTags",
                "ecs:RunInstances",
                "bss:DescribeOrderList",
                "bss:DescribeOrderDetail",
                "bss:PayOrder",
                "bss:CancelOrder"
          ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

- 脚本配置策略示例三：允许RAM用户创建了ECS实例后查询实例和块存储信息。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                    "ecs:DescribeInstances",
                    "ecs:DescribeDisks"
          ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

3. 授予RAM用户访问云服务器ECS资源的权限策略。

   具体操作，请参见为RAM用户授权。

后续步骤

完成授权后，即可以使用RAM用户登录控制台操作目标资源。具体操作，请参见RAM用户登录阿里云控制台。

4.3. 限制RAM用户创建ECS实例时创建Default VPC

通过限制CreateVpc API能够限制RAM用户创建VPC,但是在创建ECS实例时，RAM用户还是能够在没有传入VPC时由系统自动创建Default VPC和vSwitch。当您需要限制RAM用户创建ECS时创建Default VPC，可以通过访问控制RAM（Resource Access Management）的自定义策略实现。通过本文，您可以了解限制RAM用户在当前地域没有VPC时禁止创建default VPC并创建ECS操作方法。

背景信息

云服务器ECS提供了RAM用户来实现不同业务之间的隔离操作，被赋予AliyunECSFullAccess（管理ECS）权限的RAM用户默认拥有创建ECS、查看ECS、重启ECS等权限。如果您需要限制RAM用户在当前地域没有VPC时禁止创建default VPC并创建ECS的权限，同时保留其他权限，可通过访问控制RAM自定义策略来实现。查看RAM用户权限，请参见查看RAM用户的权限。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**脚本编辑**页签。
5. 输入权限策略内容，然后单击**下一步：编辑基本信息**。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "vpc:CreateDefaultVpc": [
                        "true"
                    ]
                }
            }
        }
    ]
}
```

6. 在**基本信息**区域，输入权限策略**名称**和**备注**。
7. 单击**确定**。
8. 为RAM用户授权。
   i. （可选）创建RAM用户。具体操作，请参见创建RAM用户。

      > **说明** 如果您已经创建了RAM用户，可跳过该步骤。

   ii. 在左侧导航栏，选择**身份管理 > 用户**。
   iii. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
   iv. 在**添加权限**面板，为RAM用户添加权限。

   配置项说明如下：

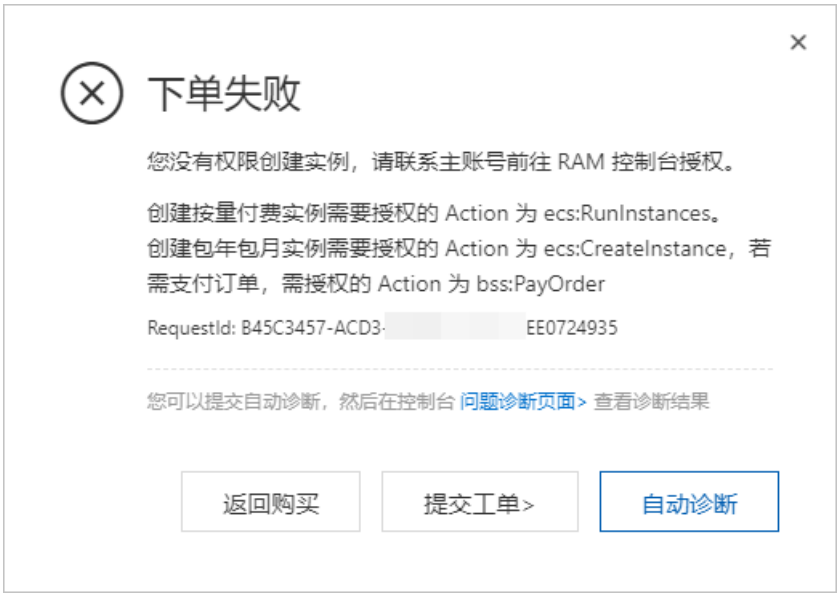
配置项	说明
授权范围	选择整个云账号，表示对应的权限应用范围为全局权限。
授权主体	系统根据您上一步选择的目标RAM用户，已自动匹配填写。
选择权限	选择自定义策略，单击您之前创建的自定义策略，将其添加到已选择的区域框中。

   v. 单击**确定**。
   vi. 单击**完成**。

执行结果

当前地域没有VPC时，该RAM用户通过控制台或API创建ECS时，具体结果如下：

- 通过控制台创建ECS时，会提示如下错误。



- 通过调用CreateInstance创建ECS，会提示如下错误。

```
7 lines
{
  "RequestId": "312F83AF-DE95- 6A637AF1",
  "HostId": "ecs.cn-guangzhou.aliyuncs.com",
  "Code": "Forbidden.RAM",
  "Message": "User not authorized to operate on the specified resource, or this API doesn't support RAM.",
  "Recommend": "https://next.api.aliyun.com/troubleshoot?q=Forbidden.RAM&product=Ecs"
}
```

4.4. 通过RAM角色控制资源访问

4.4.1. 概述

实例RAM角色允许您将一个角色关联到ECS实例，在实例内部基于STS（Security Token Service）临时凭证访问其他云产品的API，临时凭证将周期性更新。即可以保证云账号AccessKey安全，还可以借助访问控制RAM实现精细化控制和权限管理。

应用场景

ECS实例上部署的应用程序在云产品通信中，通过云账号或者RAM用户的AccessKey访问阿里云其他云产品（例如OSS、VPC、RDS等）的API。为了方便和快速地调用，部分用户直接把AccessKey固化在实例中，如写在配置文件中。这种方式存在权限过高、泄露信息和难以维护等问题。实例RAM角色能避免此类问题，例如在ECS实例中使用STS临时凭证访问阿里云的其他云服务。

ECS实例RAM（Resource Access Management）角色让ECS实例扮演具有某些权限的角色，从而赋予实例一定的访问权限。关于角色的详细描述，请参见RAM角色概览。

功能优势

使用实例RAM角色，您可以：

- 借助实例RAM角色，将角色和ECS实例关联起来。
- 使用STS临时凭证访问阿里云的其他云服务。
- 为不同的实例赋予包含不同授权策略的角色，使它们对不同的云资源具有不同的访问权限，实现更精细粒

度的权限控制。

- 无需自行在实例中保存AccessKey，通过修改角色的授权即可变更权限，快捷地维护ECS实例所拥有的访问权限。

计费详情

赋予云服务器ECS实例RAM角色不会产生额外的费用。

使用限制

使用实例RAM角色存在如下限制：

- 实例的网络类型必须是专有网络VPC。
- 一台ECS实例一次只能授予一个实例RAM角色。

相关链接

- 如果您要了解支持STS临时凭证的云服务，请参见支持RAM的云服务。
- 如果您要了解如何访问其他云产品的API，请参见借助于实例RAM角色访问其他云产品。
- 如果您要获取临时授权Token的相关信息，请参见获取临时授权Token。

4.4.2. 授予实例RAM角色

本文介绍了如何在控制台创建、授权实例RAM角色，并将其授予ECS实例。

前提条件

- 您已经开通RAM服务。更多信息，请参见开通方法。
- 待授予实例RAM角色的ECS实例网络类型必须是专有网络VPC。
- 如果您是通过RAM用户操作本文示例，您需要通过云账号授权RAM用户允许使用实例RAM角色。具体操作，请参见授权RAM用户使用实例RAM角色。

背景信息

- 一台ECS实例一次只能授予一个实例RAM角色。
- 当您给ECS实例授予了实例RAM角色后，并希望在ECS实例内部部署的应用程序中访问云产品的API时，您需要通过实例元数据获取实例RAM角色的临时授权Token。具体操作，请参见获取临时授权Token。

操作步骤

本文示例使用云账号在RAM控制台创建一个实例RAM角色，并将其授予ECS实例：

1. 步骤一：创建实例RAM角色
2. 步骤二：为RAM角色授予权限
3. 步骤三：为实例授予RAM角色

步骤一：创建实例RAM角色

按以下步骤在访问控制RAM控制台创建一个实例RAM角色：

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 角色**。
3. 在**角色**页面，单击**创建角色**。

4. 在**创建角色**面板，选择可信实体类型选择为**阿里云服务**，然后单击**下一步**。

   阿里云服务用于授权ECS实例访问或管理您的云资源。RAM角色选择**阿里云服务**类型后，支持授予给ECS实例。

> **说明**
>
> 如果您的RAM角色选择**阿里云账号**等类型，创建结束后需要在RAM角色的**信任策略管理**页签，单击**修改信任策略**手动添加以下ECS服务授权策略。

```
"Service": [
    "ecs.aliyuncs.com"
]
```

5. 选择角色类型为**普通服务角色**。
6. 输入**角色名称**和**备注**。
7. 选择受信服务为**云服务器**。
8. 单击**完成**。
9. 单击**关闭**。

配置完成后，在RAM角色的**信任策略管理**页签中，确认是否包含以下ECS服务授权策略。

步骤二：为RAM角色授予权限

按以下步骤在访问控制RAM控制台授权实例RAM角色一个系统权限或者自定义权限：

1. 使用阿里云账号登录RAM控制台。
2. （可选）如果您不使用系统权限，可以参见账号访问控制创建自定义权限策略章节创建一个自定义策略。
3. 在左侧导航栏，选择**身份管理 > 角色**。
4. 在**角色**页面，单击目标RAM角色**操作**列的**精确授权**。
5. 在**添加权限**面板，选择权限策略类型为**系统策略**或**自定义策略**，然后输入权限策略名称。

   > **说明** 您可以在左侧导航栏，选择**权限管理 > 权限策略**，在权限策略列表中查看目标权限策略名称。

6. 单击**确定**。
7. 单击**关闭**。

步骤三：为实例授予RAM角色

按以下步骤在ECS控制台为一台ECS实例授予实例RAM角色：

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到要操作的ECS实例，选择**更多 > 实例设置 > 授予/收回RAM角色**。

5. 在弹窗中，选择创建好的实例RAM角色，单击**确定**完成授予。

您也可以在创建ECS实例时，并在**系统配置**页面的**实例RAM角色**属性中为实例选择已创建好的实例RAM角色。更多信息，请参见使用向导创建实例。

相关文档

- CreateRole
- CreatePolicy
- AttachPolicyToRole
- AttachInstanceRamRole

4.4.3. 管理实例RAM角色

4.4.3.1. 更换实例RAM角色

授予了实例RAM角色后，您可以随时为ECS实例更换实例RAM角色。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 选择一个已经授予RAM角色的ECS实例，选择**更多 > 实例设置 > 授予/收回RAM角色**。

5. **操作类型**选择**授予**，在已有**RAM 角色**中选择其他实例RAM角色，单击**确定**即可更换当前RAM角色。

相关文档

- AttachInstanceRamRole

4.4.3.2. 收回实例RAM角色

授予了实例RAM角色后，您可以随时为ECS实例收回实例RAM角色。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 选择一个已经授予RAM角色的ECS实例，选择**更多 > 实例设置 > 授予/收回RAM角色**。

5. **操作类型**选择**收回**，单击**确定**即可收回实例RAM角色。

相关文档

- DetachInstanceRamRole

4.4.3.3. 获取临时授权Token

您可以获得实例RAM角色的临时授权Token，该临时授权Token可以执行实例RAM角色的权限和资源，并且该临时授权Token会自动周期性地更新。

操作步骤

1. 远程连接ECS实例。连接方式请参见连接方式概述ECS远程连接操作指南。
2. 检索实例RAM角色的临时授权Token。假设实例RAM角色的名称为 `EcsRamRoleDocumentTesting` 。
   - Linux实例执行以下命令：

- Linux实例执行以下命令：

```
curl http://100.100.100.200/latest/meta-data/ram/security-credentials/EcsRamRoleDocumentTesting
```

- Windows实例执行以下PowerShell命令：

```
Invoke-RestMethod http://100.100.100.200/latest/meta-data/ram/security-credentials/EcsRamRoleDocumentTesting
```

获得临时授权Token，返回示例如下所示。

```
{
   "AccessKeyId" : "<yourAccessKeyId>",
   "AccessKeySecret" : "<yourAccessKeySecret>",
   "Expiration" : "2017-11-01T05:20:01Z",
   "SecurityToken" : "<yourSecurityToken>",
   "LastUpdated" : "2017-10-31T23:20:01Z",
   "Code" : "Success"
}
```

相关文档

- ECS实例元数据概述

4.4.3.4. 授权RAM用户使用实例RAM角色

如果您需要通过RAM用户授予、更换、收回实例RAM角色，您需要通过阿里云账号授权RAM用户允许使用实例RAM角色。本文操作仅适用于阿里云账号。

背景信息

当您授权RAM用户使用实例RAM角色时，您必须授权RAM用户对该实例RAM角色的PassRole权限。其中，PassRole决定该RAM用户能否直接执行角色策略赋予的权限。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
4. 在**添加权限**面板，为RAM用户添加权限。
   i. 选择授权应用范围。
      - **整个云账号**：权限在当前阿里云账号内生效。
      - **指定资源组**：权限在指定的资源组内生效。

        > **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

   ii. 输入授权主体。

   授权主体即需要授权的RAM用户，系统会自动填入当前的RAM用户，您也可以添加其他RAM用户。

   iii. 在**选择权限**区域，单击**新建权限策略**。

iv. 选择脚本编辑，新建自定义权限策略。

自定义策略如下所示，其中，[ECS RAM Action]表示可授权RAM用户的权限，更多取值请参见鉴权规则。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs: [ECS RAM Action]",
                "ecs: CreateInstance",
                "ecs: AttachInstanceRamRole",
                "ecs: DetachInstanceRAMRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ram:PassRole",
            "Resource": "*"
        }
    ]
}
```

5. 返回**添加权限**面板，在**选择权限**区域单击**自定义策略**。
6. 在左侧**权限策略名称**列表下，单击需要授予RAM用户的自定义权限策略。

> **说明** 在右侧区域框，选择某条策略并单击×，可撤销该策略。

7. 单击**确定**。
8. 单击**完成**。

相关文档

- CreatePolicy
- AttachPolicyToRole

4.4.4. 通过API使用实例RAM角色

您可以通过API创建、授权实例RAM角色，并将其授予实例。

前提条件

请确保您已经开通RAM服务。更多信息，请参见开通方法。

背景信息

使用限制如下：

- 只有专有网络（VPC）网络类型的ECS实例才能使用实例RAM角色。
- 一个ECS实例一次只能授予一个实例RAM角色。

- 当您给ECS实例授予了实例RAM角色后，并希望在ECS实例内部部署的应用程序中访问云产品的API时，您需要通过实例元数据获取实例RAM角色的临时授权Token。更多信息，请参见获取临时授权Token。
- 如果您是通过RAM用户使用实例RAM角色，您需要通过阿里云账号授权RAM用户使用实例RAM角色。具体操作，请参见授权RAM用户使用实例RAM角色。

操作步骤

通过API使用实例RAM角色的操作步骤如下：

1. 步骤一：创建实例RAM角色
2. 步骤二：授权实例RAM角色
3. 步骤三：授予实例RAM角色
4. 步骤四：（可选）收回实例RAM角色
5. 步骤五：（可选）获取临时授权Token
6. 步骤六：（可选）授权RAM用户使用实例RAM角色

步骤一：创建实例RAM角色

调用CreateRole接口创建实例RAM角色。

设置RoleName参数，例如将其值置为*EcsRamRoleDocumentTesting*。

按如下策略设置参数AssumeRolePolicyDocument：

```
{
     "Statement": [
     {
         "Action": "sts:AssumeRole",
         "Effect": "Allow",
         "Principal": {
         "Service": [
         "ecs.aliyuncs.com"
         ]
         }
     }
     ],
     "Version": "1"
 }
```

步骤二：授权实例RAM角色

1. 调用CreatePolicy接口新建授权策略。

   设置如下参数：

   - 设置RoleName参数，例如*EcsRamRoleDocumentTestingPolicy*。
   - 按如下策略设置参数PolicyDocument：

```
{
     "Statement": [
         {
         "Action": [
             "oss:Get*",
             "oss:List*"
         ],
         "Effect": "Allow",
         "Resource": "*"
         }
     ],
     "Version": "1"
 }
```

2. 调用AttachPolicyToRole接口授权角色策略。

   设置如下参数：

   - 设置PolicyType参数为*Custom*。
   - 设置PolicyName参数，例如*EcsRamRoleDocumentTestingPolicy*。
   - 设置RoleName参数，例如*EcsRamRoleDocumentTesting*。

步骤三：授予实例RAM角色

调用AttachInstanceRamRole接口为实例授予RAM角色。

设置如下参数：

- 设置RegionId及InstanceIds参数指定一个ECS实例。
- 设置RamRoleName参数，例如*EcsRamRoleDocumentTesting*。

步骤四：（可选）收回实例RAM角色

调用DetachInstanceRamRole接口收回实例RAM角色。

设置如下参数：

- 设置RegionId及InstanceIds参数指定一个ECS实例。
- 设置RamRoleName参数，例如*EcsRamRoleDocumentTesting*。

步骤五：（可选）获取临时授权Token

您可以获得实例RAM角色的临时授权Token，该临时授权Token可以执行实例RAM角色的权限和资源，并且该临时授权Token会自动周期性地更新。操作步骤如下：

检索名为EcsRamRoleDocumentTesting的实例RAM角色的临时授权Token。

- Linux实例：执行命令 `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` 。
- Windows实例：具体操作，请参见实例元数据。

获得临时授权Token。返回示例如下：

```
{
"AccessKeyId" : "XXXXXXXXX",
"AccessKeySecret" : "XXXXXXXXX",
"Expiration" : "2017-11-01T05:20:01Z",
"SecurityToken" : "XXXXXXXXX",
"LastUpdated" : "2017-10-31T23:20:01Z",
"Code" : "Success"
}
```

步骤六：（可选）授权RAM用户使用实例RAM角色

> **说明** 当您授权RAM用户使用实例RAM角色时，您必须授权RAM用户对该实例RAM角色的PassRole权限。其中，PassRole决定该RAM用户能否直接执行角色策略赋予的权限。

1. 登录RAM控制台。
2. 授权RAM用户使用实例RAM角色。具体操作，请参见为RAM用户授权。

```
{
        "Version": "2016-10-17",
        "Statement": [
            {
            "Effect": "Allow",
            "Action": [
                "ecs: [ECS RAM Action]",
                "ecs: CreateInstance",
                "ecs: AttachInstanceRamRole",
                "ecs: DetachInstanceRAMRole"
            ],
            "Resource": "*"
            },
            {
        "Effect": "Allow",
        "Action": "ram:PassRole",
        "Resource": "*"
            }
        ]
}
```

其中，*[ECS RAM Action]*表示可授权RAM用户的权限。更多信息，请参见鉴权规则。

相关文档

相关文档

- 授予实例RAM角色
- 使用实例RAM角色访问其他云产品
- CreateRole
- ListRoles
- CreatePolicy
- AttachPolicyToRole

- AttachInstanceRamRole
- DetachInstanceRamRole
- DescribeInstanceRamRole

4.5. 系统策略示例

本文列出云服务器ECS常用系统策略的详情，供您了解权限策略涉及的操作等信息，您也可以按需自定义权限策略。

AliyunECSFullAccess

管理云服务器ECS相关资源的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": "ecs:*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSReadOnlyAccess

查看云服务器ECS相关资源的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": "ecs:Describe*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ecs:List*",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSNetworkInterfaceManagementAccess

管理弹性网卡的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "vpc:DescribeVSwitchAttributes"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:CreateNetworkInterface",
                "ecs:DeleteNetworkInterface",
                "ecs:DescribeNetworkInterfaces",
                "ecs:CreateNetworkInterfacePermission",
                "ecs:DescribeNetworkInterfacePermissions",
                "ecs:DeleteNetworkInterfacePermission"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSAssistantFullAccess

管理云助手命令的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:*Command",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:StopInvocation",
                "ecs:*CloudAssistant*"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

AliyunECSAssistantReadonlyAccess

查看云助手命令的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeInstances",
                "ecs:DescribeTag*",
                "ecs:DescribeCommand*",
                "ecs:DescribeInvocation*",
                "ecs:DescribeCloudAssistant*"
            ],
            "Resource": [
                "acs:ecs:*:*:instance/*",
                "acs:ecs:*:*:command/*"
            ]
        }
    ]
}
```

AliyunECSImageExportRolePolicy

导出ECS实例镜像的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:GetObject",
                "oss:PutObject",
                "oss:DeleteObject",
                "oss:GetBucketLocation",
                "oss:AbortMultipartUpload",
                "oss:ListMultipartUploads",
                "oss:ListParts",
                "oss:GetBucketInfo",
                "oss:GetBucketUserQos"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSImageImportRolePolicy

导入镜像的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:GetObject",
                "oss:GetBucketLocation",
                "oss:GetBucketInfo"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AliyunECSInstanceForYundunSysTrustRolePolicy

安全增强型实例可信服务的权限策略详情：

```
{
    "Statement": [
        {
            "Action": [
                "yundun-systrust:GenerateNonce",
                "yundun-systrust:GenerateAikcert",
                "yundun-systrust:RegisterMessage",
                "yundun-systrust:PutMessage"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ],
    "Version": "1"
}
```

AliyunECSDiskEncryptRolePolicy

加密云盘的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "kms:List*",
                "kms:DescribeKey",
                "kms:TagResource",
                "kms:UntagResource"
            ],
            "Resource": [
                "acs:kms:*:*:*",
                "acs:kms:*:*:*/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "acs:kms:*:*:*/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AliyunServiceRolePolicyForECSAutoProvisioning

弹性供应功能的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:CreateInstance",
                "ecs:RunInstances",
                "ecs:StartInstance",
                "ecs:AllocatePublicIpAddress",
                "ecs:StopInstance",
                "ecs:DeleteInstance",
                "ecs:DescribeInstances",
                "ecs:DescribeInstanceAttribute",
                "ecs:ModifyInstanceAttribute",
                "ecs:DescribeSecurityGroupAttribute",
                "ecs:DescribeImages",
                "ecs:DescribeSnapshots",
                "ecs:DescribeKeyPairs",
                "ecs:CreateLaunchTemplate",
                "ecs:DescribeLaunchTemplates",
                "ecs:DescribeLaunchTemplateVersions",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeHpcClusters",
                "ecs:DescribeImageFromFamily",
                "slb:DescribeLoadBalancerAttribute",
                "slb:RemoveBackendServers",
                "slb:DescribeHealthStatus",
                "slb:AddBackendServers",
                "slb:SetBackendServers",
                "slb:DescribeLoadBalancers",
                "slb:DescribeVServerGroups",
                "slb:DescribeVServerGroupAttribute",
                "slb:AddVServerGroupBackendServers",
                "slb:RemoveVServerGroupBackendServers",
                "slb:DescribeMasterSlaveServerGroupAttribute",
                "slb:DescribeMasterSlaveServerGroups",
                "slb:SetVServerGroupAttribute",
                "slb:DescribeLoadBalancerUDPListenerAttribute",
                "slb:DescribeLoadBalancerHTTPListenerAttribute",
                "slb:DescribeLoadBalancerHTTPSListenerAttribute",
                "slb:DescribeLoadBalancerTCPListenerAttribute",
                "rds:ModifySecurityIps",
                "rds:DescribeDBInstanceAttribute",
                "rds:DescribeTaskInfo",
                "rds:DescribeDBInstanceIPArrayList",
                "oos:GetTemplate",
                "oos:StartExecution",
                "ecs:DescribeUserData",
                "ecs:DescribeInstanceRamRole",
                "ecs:DescribeDisks",
                "ecs:DescribeAutoSnapshotPolicyEx",
                "ecs:DescribeDedicatedHosts",
                "ecs:DescribeDedicatedHostTypes"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "mns:ListTopic",
                "mns:ListQueue",
                "mns:SendMessage",
                "mns:PublishMessage"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cms:NodeInstall",
                "cms:NodeStatusList",
                "cms:QueryCustomMetricList",
                "cms:ProfileSet",
                "cms:CreateAlert",
                "cms:DeleteAlert",
                "cms:QueryAlert",
                "cms:UpdateAlert",
                "cms:DisableAlert",
                "cms:EnableAlert",
                "cms:CreateAction",
                "cms:GetAction",
                "cms:CreateDimensions",
                "cms:QueryDimensions",
                "cms:UpdateDimensions",
                "cms:QueryMetricList",
                "cms:ListAlarmHistory"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:PassRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "acs:Service": [
                        "ecs.aliyuncs.com",
                        "oos.aliyuncs.com"
                    ]
```

```
                }
            }
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "autoprovisioning.ecs.aliyuncs.com"
                }
            }
        }
    ]
}
```

AliyunServiceRolePolicyForECSImageBuilder

镜像构建功能的权限策略详情：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oos:CreateTemplate",
                "oos:StartExecution",
                "oos:CancelExecution",
                "oos:ListExecutions",
                "oos:ListTaskExecutions",
                "oos:ListExecutionLogs",
                "oos:DeleteTemplate"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ecs:DescribeAvailableResource",
                "ecs:DescribeInstances",
                "ecs:DescribeCloudAssistantStatus",
                "ecs:DescribeImages",
                "ecs:DescribeInvocations",
                "ecs:DescribeInvocationResults",
                "ecs:CreateSecurityGroup",
                "ecs:DescribeSecurityGroups",
                "ecs:CancelCopyImage",
                "ecs:RunInstances",
                "ecs:CopyImage",
                "ecs:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
        {
            "Action": [
                "ecs:RebootInstance",
                "ecs:DeleteInstance",
                "ecs:DeleteImage",
                "ecs:DescribeImageSharePermission",
                "ecs:DeleteSecurityGroup",
                "ecs:ModifyImageSharePermission",
                "ecs:InstallCloudAssistant",
                "ecs:RunCommand",
                "ecs:StopInstance",
                "ecs:CreateImage"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ecs:tag/imagepipelineid": "*"
                }
            }
        },
        {
            "Action": [
                "vpc:DescribeVSwitches",
                "vpc:DescribeVpcs",
                "vpc:CreateVpc",
                "vpc:CreateVSwitch",
                "vpc:DeleteVSwitch",
                "vpc:DeleteVpc"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "imagebuilder.ecs.aliyuncs.com"
                }
            }
        }
    ]
}
```

5.DDoS基础防护

DDoS基础防护服务可以有效防止云服务器ECS实例受到恶意攻击，从而保证ECS系统的稳定，即当流入ECS实例的流量超出实例规格对应的限制时，云盾就会帮助ECS实例限流，避免ECS系统出现问题。

阿里云云盾默认为ECS实例免费提供最大5 Gbit/s的流量攻击的防护，不同实例规格的免费防护流量不同，您可以登录云盾DDoS防护管理控制台查看实际防护阈值。更多信息，请参见DDoS基础防护黑洞阈值。

DDoS基础防护工作原理

启用DDoS基础防护后，云盾会实时监控进入ECS实例的流量。当监测到超大流量或者包括DDoS攻击在内的异常流量时，在不影响正常业务的前提下，云盾会将可疑流量从原始网络路径中重定向到净化产品上，识别并剥离恶意流量，并将还原的合法流量回注到原始网络中转发给目标ECS实例。这一过程，就是流量清洗。更多信息，请参见什么是DDoS原生防护。

> **说明** 启用了DDoS基础防护的ECS实例，当来自互联网的流量大于5 Gbit/s时，为保护整个集群的安全，阿里云会让相应ECS实例进入黑洞，丢弃进入该实例的所有流量，屏蔽公网对它的所有访问。更多信息，请参见DDoS防护指南-阿里云黑洞策略。

流量清洗的触发条件包括：

- 流量模型的特征。当流量符合攻击流量特征时，就会触发清洗。
- 流量大小。DDoS攻击一般流量都非常大，通常都以Gbit/s为单位，因此，当进入ECS实例的流量达到设置的阈值时，无论是否为正常业务流量，云盾都会启动流量清洗。

流量清洗的方法包括：过滤攻击报文、限制流量速度、限制数据包速度等。

所以，在使用DDoS基础防护时，您需要设置以下阈值：

- BPS清洗阈值：当入方向流量超过BPS清洗阈值时，会触发流量清洗。
- PPS清洗阈值：当入方向数据包数超过PPS清洗阈值时，会触发流量清洗。

清洗阈值以控制台显示为准，具体操作，请参见资产中心。示例如下图所示。

相关操作

云服务器ECS默认开启DDoS基础防护。ECS实例创建后，您可以执行以下操作：

- 设置清洗阈值：ECS实例创建后，默认按实例规格对应的最大阈值执行DDoS基础防护。但是，部分实例规格的最大清洗阈值（BPS）可能过大，无法起到应有的防护作用，所以，您需要根据实际情况调整清洗阈值，具体操作，请参见DDoS基础防护用户指南-DDos基础防护设置。
- （不推荐）取消流量清洗：当进入ECS实例的流量达到清洗阈值时，无论是否为正常业务流量，云盾都会启动流量清洗，此时，可能会导致正常业务不可用或受影响。为了保证正常业务，您可以手动取消流量清洗。具体操作，请参见DDos基础防护用户指南-如何取消流量清洗。

> **警告** 取消流量清洗后，当流入ECS实例的流量超过对应的黑洞阈值（最大为5 Gbit/s）时，您的ECS实例会进入黑洞。请谨慎操作。

6.基础安全服务

云服务器ECS提供了基础安全服务，包括异常登录检测、漏洞扫描、基线配置核查等。您可以在ECS控制台或者云安全中心看到您的云服务器安全状态。

背景信息

由阿里云云安全中心（Security Center）提供云服务器ECS的基础安全服务，帮助您收集并呈现安全日志和云上资产指纹，主要提供免费版的漏洞检测、安全告警和基线检查服务。您可以在ECS管理控制台的**概览**页面或者云安全中心控制台查看相关安全信息。更多信息，请参见云安全中心产品文档。

基础安全服务的计费方式如下：

- 云服务器ECS的基础安全服务为免费服务，不收取服务费用。
- 如果您需要升级为高级版或者企业版云安全中心，可以在云安全中心控制台免费试用或者购买服务。高级版或者企业版云安全中心的计费方式请参见 *云安全中心文档*计费模式。

使用安全插件Agent

云安全中心的安全插件Agent是安装在云服务器ECS中的低损耗的控件。未安装Agent的云服务器ECS不会受到云安全中心保护，ECS管理控制台页面也不会显示该资产的漏洞、告警、基线漏洞和资产指纹等数据。关于Agent的安装路径，请参见Agent概述。

您可以按以下方式操作Agent。

- 创建ECS实例时自动安装Agent
  i. 登录ECS管理控制台。
  ii. 在左侧导航栏，选择**实例与镜像 > 实例**。
  iii. 在顶部菜单栏处，选择地域。
  iv. 创建一台ECS实例，在**镜像**区域，选中**安全加固**，系统自动为新建ECS实例安装Agent。更多信息，请参见使用向导创建实例。

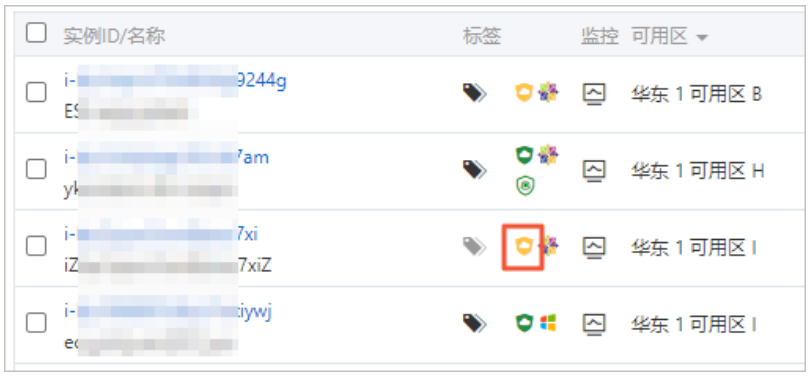
> **说明** 您也可以在调用RunInstances时通过设置 `SecurityEnhancementStrategy=Active` 为新建ECS实例自动安装Agent。

- 为已有的ECS实例手动安装Agent
  i. 登录ECS管理控制台。
  ii. 在**概览**页面，单击**安全评分**中的**立即处理**，前往云安全中心管理控制台。
  iii. 安装Agent。具体操作，请参见 *云安全中心文档*安装Agent。
- 卸载Agent
  i. 登录ECS管理控制台。
  ii. 在**概览**页面，单击**安全评分**中的**立即处理**，前往云安全中心管理控制台。
  iii. 卸载Agent。具体操作，请参见 *云安全中心文档*卸载Agent。

查看安全状态

您可以按以下步骤查看云服务器ECS的安全状态。

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 根据需要选择以下一种方式查看安全状态：
   - 方式一：在**实例列表**页面查看基础安全服务的状态。橙色云盾图标表示ECS实例有漏洞告警或安全告警等，您可以单击图标进入云安全中心控制台查看告警详情。

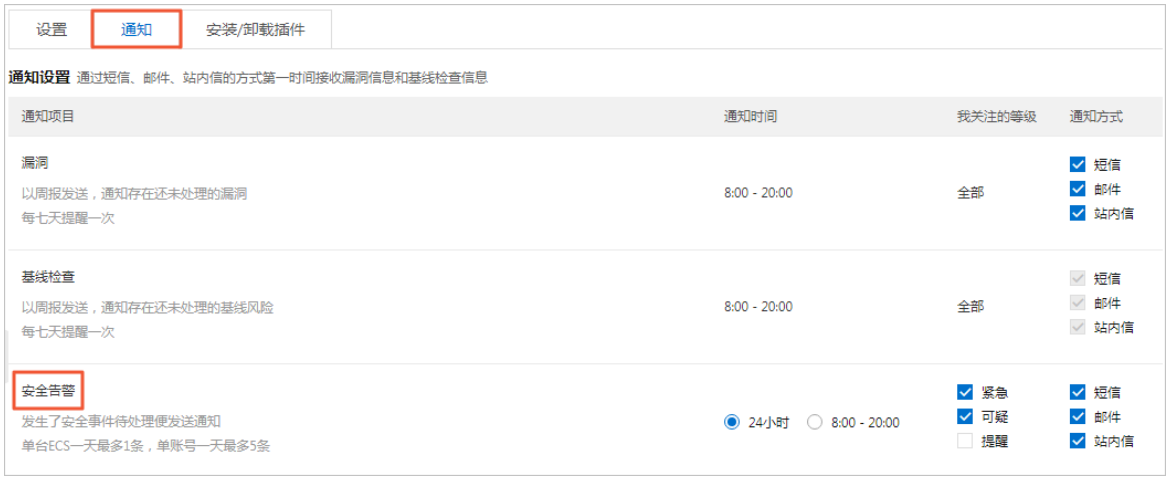


   - 方式二：单击实例ID进入**实例详情**页面，在**实例详情**页面中查看基础安全服务的状态。您可以单击图标进入云安全中心控制台查看告警详情。

设置告警通知

基础安全服务支持对安全告警处理项目设置告警通知，接收方式包括短信、邮件和站内信。您可以按以下方式设置告警通知。

1. 登录ECS管理控制台。
2. 在**概览**页面，单击**安全评分**中的**立即处理**，前往云安全中心管理控制台。
3. 在左侧导航栏，单击**设置**，然后在**设置**页面中单击**通知**页签。
4. 在**安全告警**区域，选择消息等级，设置通知方式和通知时间。



说明 如果您已经升级为高级版或者企业版云安全中心，请参见 *云安全中心文档*安全告警概述查看更多告警方式。

相关文档

相关文档

- 云安全中心基础版、高级版和企业版功能对比
-
- RunInstances

7.安全FAQ

本文汇总了云服务器ECS安全方面的常见问题。

- 安全组问题
  - 什么是安全组？
  - 为什么要在创建ECS实例时选择安全组？
  - 创建ECS实例前，未创建安全组怎么办？
  - 为什么ECS实例加入安全组时提示规则数量超限？
  - 专有网络VPC类型ECS实例的安全组数量上限调整后，只对调整日期后新增的安全组生效吗？
  - 安全组在什么情况下会使用默认安全组规则？
  - 不同安全组的ECS实例如何实现内网互通？
  - 同一安全组的ECS实例如何实现内网隔离？
  - 为什么我配置安全组后还是无法访问服务？
  - 弹性网卡如何加入到安全组？
- 安全组规则问题
  - 什么场景下我需要添加安全组规则？
  - 安全组规则中协议和端口之间是什么关系？
  - 安全组规则授权对象中的IP地址和CIDR地址块是什么关系？
  - 为什么无法访问TCP 25端口？
  - 为什么无法访问80端口？
  - 为什么安全组里自动添加了很多内网相关的安全组规则？
  - 安全组规则配置错误会造成什么影响？
  - 安全组的入方向规则和出方向规则区分计数吗？
  - 是否可以调整安全组规则的数量上限？
  - 我配置的安全组规则，各规则的优先级排序是怎么样的？
- 主机处罚与解禁问题
  - 收到违法阻断网站整改通知，怎么办？
  - 收到对外攻击需要整改的通知，怎么办？
- 限额问题
  - 如何查看资源的限额？
  - 提高VPC网络普通安全组组内IP地址上限，目前已经在哪些地域发布支持？

什么是安全组？

安全组是一种虚拟防火墙。用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，您可以在云端划分安全域。

每台ECS实例至少属于一个安全组，在创建实例的时候必须指定安全组。安全组类型分为普通安全组和企业安全组，详情请参见安全组概述。

为什么要在创建ECS实例时选择安全组？

在创建ECS实例之前，必须选择安全组来划分应用环境的安全域，授权安全组规则进行合理的网络安全隔离。

如果您在创建ECS实例时不选择安全组，创建的ECS实例会分配到一个固定的安全组（即默认安全组），建议您将实例移出默认安全组并加入新的安全组来实现网络安全隔离。

创建ECS实例前，未创建安全组怎么办？

如果您在创建ECS实例前，未创建安全组，您可以选择默认安全组。默认的安全组放行了常用端口，如TCP 22端口、3389端口等。

为什么ECS实例加入安全组时提示规则数量超限？

作用于一台ECS实例（主网卡）的安全组规则数量上限 = 该实例允许加入的安全组数量 * 每个安全组最大规则数量。

如果提示**加入安全组失败，作用在该实例上的安全组规则数量已达上限**，表示当前ECS实例上的规则总数已经超过数量上限。建议您重新选择安全组。

专有网络VPC类型ECS实例的安全组数量上限调整后，只对调整日期后新增的安全组生效吗？

不是。该上限调整对调整日期之前和之后创建的所有专有网络VPC类型ECS实例的安全组都生效。

安全组在什么情况下会使用默认安全组规则？

在以下情况中会使用默认安全组规则：

- 通过ECS管理控制台在一个地域首次创建ECS实例时，如果您尚未创建安全组，可以选择系统自动创建的默认安全组，类型为普通安全组。默认安全组采用默认安全规则。入方向放行ICMP协议、SSH 22端口、RDP 3389端口，授权对象为全网段（0.0.0.0/0），优先级为100，您还可以勾选放行HTTP 80端口和HTTPS 443端口。出方向允许所有访问。
- 您在ECS管理控制台上创建安全组时默认的安全组规则，入方向放行ICMP协议、SSH 22端口、RDP 3389端口、HTTP 80端口和HTTPS 443端口，授权对象为全网段（0.0.0.0/0）。

不同安全组的ECS实例如何实现内网互通？

同一账号或者不同账号下两个安全组之间的实例默认内网都是隔离的。不同安全组之间实现内网互通的应用案例，请参见不同安全组的实例内网互通和经典网络内网实例互通设置方法。

同一安全组的ECS实例如何实现内网隔离？

加入同一个普通安全组内的实例之间默认允许所有协议、端口互相访问，您可以修改普通安全组内的网络连通策略，实现组内隔离。更多信息，请参见普通安全组内网络隔离。

为什么我配置安全组后还是无法访问服务？

控制台安全组放行某个端口，只能说明安全组没有限制这个端口的访问，不能说明这个端口已经开启。如需外网访问ECS服务器的端口需要满足以下三个必要条件：

- 安全组规则放行该端口。
- 对应端口的程序软件是启动运行状态，并且监听地址为0.0.0.0（您可通过执行**netstat -ano |findstr 端口号**命令来检测端口是否处于监听状态）。
- 已关闭ECS实例内部防火墙，或者防火墙已放行该端口。

弹性网卡如何加入到安全组？

您可以通过变更ECS实例所在的安全组来更新弹性网卡主网卡的安全组，也可以修改辅助弹性网卡的属性来修改弹性网卡所属的安全组。具体操作，请参见修改弹性网卡。

什么场景下我需要添加安全组规则？

在以下场景中，您需要添加安全组规则，保证ECS实例能被正常访问：

- ECS实例所在的安全组没有添加过安全组规则，也没有默认安全组规则。当ECS实例需要访问公网，或访问当前地域下其他安全组中的ECS实例时，您需要添加安全规则。
- 搭建的应用没有使用默认端口，而是自定义了一个端口或端口范围。此时，您必须在测试应用连通前放行自定义的端口或端口范围。例如，您在ECS实例上搭建Nginx服务时，通信端口选择监听在TCP 8000，但您的安全组只放行了80端口，则您需要添加安全规则，保证Nginx服务能被访问。
- 其他场景，请参见安全组应用案例ECS安全组配置操作指南。

安全组规则中协议和端口之间是什么关系？

添加安全组规则时，您必须指定通信端口或端口范围，然后安全组根据允许或拒绝策略决定是否转发数据到ECS实例。

安全组规则中协议和端口信息如下表所示。更多端口信息，请参见典型应用的常用端口。

协议类型	端口显示范围	应用场景
全部	-1/-1，表示不限制端口。不支持设置。	可用于完全互相信任的应用场景。
全部 ICMP（IPv4）	-1/-1，表示不限制端口。不支持设置。	使用 `ping` 程序检测ECS实例之间的通信状况。
全部 GRE	-1/-1，表示不限制端口。不支持设置。	用于VPN服务。
自定义 TCP	自定义端口范围，有效的端口值是1 ~ 65535。 必须采用*<开始端口>/<结束端口>*的格式。例如80/80表示端口80，1/22表示1到22端口。	可用于允许或拒绝一个或几个连续的端口。
自定义 UDP	自定义端口范围，有效的端口值是1 ~ 65535。 必须采用*<开始端口>/<结束端口>*的格式。例如80/80表示端口80，1/22表示1到22端口。	可用于允许或拒绝一个或几个连续的端口。

其中，TCP协议类型端口的常用应用场景如下表所示。

应用场景	协议类型	端口显示范围	说明
连接服务器	SSH	22/22	用于SSH远程连接到Linux实例。连接ECS实例后您能修改端口号，具体操作，请参见修改服务器默认远程端口。
	TELNET	23/23	用于Telnet远程登录ECS实例。

应用场景	协议类型	端口显示范围	说明
	RDP	3389/3389	用于通过远程桌面协议连接到Windows实例。连接ECS实例后您能修改端口号，具体操作，请参见修改服务器默认远程端口。
网站服务	HTTP	80/80	ECS实例作为网站或Web应用服务器。
	HTTPS	443/443	ECS实例作为支持HTTPS协议的网站或Web应用服务器。
数据库	MS SQL	1433/1433	ECS实例作为MS SQL服务器。
	Oracle	1521/1521	ECS实例作为Oracle SQL服务器。
	MySQL	3306/3306	ECS实例作为MySQL服务器。
	PostgreSQL	5432/5432	ECS实例作为PostgreSQL服务器。
	Redis	6379/6379	ECS实例作为Redis服务器。

安全组规则授权对象中的IP地址和CIDR地址块是什么关系？

IP地址是单一的IP地址，例如192.168.0.100、2408:4321:180:1701:94c7:bc38:3bfa:。CIDR地址块是IP地址段，例如192.168.0.0/24、2408:4321:180:1701:94c7:bc38:3bfa:***/128。

CIDR（Classless Inter-Domain Routing）是互联网中一种新的寻址方式，与传统的A类、B类和C类寻址模式相比，CIDR在IP地址分配方面更为高效。CIDR采用斜线记法，表示为：IP地址/网络ID的位数。

- 示例一：CIDR格式换算为IP地址网段

  例如10.0.0.0/8，换算为32位二进制地址：00001010.00000000.00000000.00000000。其中/8表示8位网络ID，即32位二进制地址中前8位是固定不变的，对应网段为：00001010.00000000.00000000.00000000~00001010.11111111.11111111.11111111。则换算为十进制后，10.0.0.0/8表示：子网掩码为255.0.0.0，对应网段为10.0.0.0~10.255.255.255。

- 示例二：IP地址网段换算为CIDR格式

  例如192.168.0.0~192.168.31.255，后两段IP换算为二进制地址：00000000.00000000~00011111.11111111，可以得出前19位（8*2+3）是固定不变的，则换算为CIDR格式后，表示为：192.168.0.0/19。

为什么无法访问TCP 25端口？

TCP 25端口是默认的邮箱服务端口。基于安全考虑，云服务器ECS的25端口默认受限。建议您使用465端口发送邮件。更多应用，请参见安全组应用案例。

为什么无法访问80端口？

如何排查80端口故障，请参见检查TCP 80端口是否正常工作。

为什么安全组里自动添加了很多内网相关的安全组规则？

以下两种情况，可能导致您的安全组里自动添加了很多规则：

- 如果您访问过DMS，安全组中就会自动添加相关的规则。
- 如果您近期通过阿里云数据传输DTS功能迁移过数据，安全组中会自动添加DTS的服务IP地址相关的规则。

安全组规则配置错误会造成什么影响？

安全组配置错误会导致ECS实例在私网或公网与其他设备之间的访问失败，例如：

- 无法从本地远程连接（SSH）Linux实例或者远程桌面连接Windows实例。
- 无法远程 `ping` ECS实例的公网IP。
- 无法通过HTTP或HTTPS协议访问ECS实例提供的Web服务。
- 无法通过内网访问其他ECS实例。

安全组的入方向规则和出方向规则区分计数吗？

不区分。每个安全组的入方向规则与出方向规则的总数不能超过200。详情请参见使用限制。

是否可以调整安全组规则的数量上限？

不可以，每个安全组最多可以包含200条安全组规则。一台ECS实例中的每个弹性网卡默认最多可以加入5个安全组，所以一台ECS实例的每个弹性网卡最多可以包含1000条安全组规则，能够满足绝大多数场景的需求。

如果当前数量上限无法满足您的使用需求，建议您按照以下步骤操作：

1. 检查是否存在冗余规则。您也可以提交工单，阿里云技术支持将提供检查服务。
2. 如果存在冗余规则，请清除冗余规则。如果不存在冗余规则，您可以创建多个安全组。

如果您已开通了云防火墙服务，也可以通过云防火墙创建VPC边界访问控制策略（管控两个VPC间的流量），减少ECS安全组规则的数量。有关VPC边界防火墙的详细内容，请参见VPC边界防火墙。

我配置的安全组规则，各规则的优先级排序是怎么样的？

优先级的取值范围为1~100，数值越小，代表优先级越高。

同类型规则间依赖优先级决定最终执行的规则。当ECS实例加入了多个安全组时，多个安全组会从高到低依次匹配规则。最终生效的安全组规则如下：

- 如果两条安全组规则只有授权策略不同：拒绝策略的规则生效，允许策略的规则不生效。
- 如果两条安全组规则只有优先级不同：优先级高的规则生效。

收到违法阻断网站整改通知，怎么办？

在互联网有害信息记录中，您可以查看存在有害信息的域名或URL、处罚动作、处罚原因及处罚时间。您在确认该域名或URL中的有害信息已经移除或不存在时，可以申请解除访问封禁。详情请参见互联网有害信息。

收到对外攻击需要整改的通知，怎么办？

在处罚记录中，您可以查看详细的处罚结果、处罚原因及处罚时段。如果您不认同处罚结果，可以反馈申诉。收到您的处罚记录反馈后，阿里云将再次核验，确认处罚的正确性和有效性，并判断是否继续维持处罚或立即结束处罚。详情请参见处罚列表。

如何查看资源的限额？

查看资源的使用限制和限额，请参见使用限制。

提高VPC网络普通安全组组内IP地址上限，目前已经在哪些地域发布支持？

当VPC网络类型的普通安全组组内能容纳的私网IP地址数量达到上限2,000时，支持自助申请提高到6,000。目前该功能正在按地域陆续发布中，支持的地域如下表所示：

地域	支持申请/预期支持申请日期
阿联酋（迪拜）	已支持申请
英国（伦敦）	已支持申请
印度（孟买）	已支持申请
马来西亚（吉隆坡）	已支持申请
西南1（成都）	已支持申请
日本（东京）	已支持申请
新加坡	已支持申请
美国（硅谷）	已支持申请
澳大利亚	已支持申请
华北6（乌兰察布）	已支持申请
华南3（广州）	已支持申请
印度尼西亚（雅加达）	2022.07.11
菲律宾（马尼拉）	2022.07.13
华北 5（呼和浩特）	2022.07.15
华北 1（青岛）	2022.07.18
华南1（深圳）	2022.07.20
中国（香港）	2022.07.22
华南2（河源）	2022.07.25
华北2（北京）	2022.07.27
华东2（上海）	2022.08.03
华北 3（张家口）	2022.08.10
华东1（杭州）	2022.08.17

说明

- 表格中的预期支持申请日期仅供参考，具体以实际功能上线时间为准。
- 表格未列出所有阿里云地域，如果您在未列出的地域中有申请需求，可以提交工单咨询预期开放日期。