阿里云
云服务器 ECS

安全

文档版本：20191114

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。
*## *	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 安全组

1.1 安全组概述

安全组是一种虚拟防火墙，具备状态检测和数据包过滤功能，用于在云端划分安全域。您可以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。

安全组特点

安全组由同一个地域内具有相同安全保护需求并相互信任的ECS实例组成。安全组具有以下功能特点：

- **在创建ECS实例时必须指定安全组，每台ECS实例至少属于一个安全组。**
- **同一安全组内的ECS实例之间默认内网网络互通。**
- **在没有设置允许访问的安全组规则的情况下，不同安全组内的ECS实例默认内网不通。**
- **（仅普通安全组）可以通过安全组规则授权两个安全组之间互访。**
- **安全组具有状态检测能力，支持有状态服务，并且通过会话保持状态。如果数据包在出方向是被允许的，那么对应的此连接在入方向也是允许的。从ECS实例内发起请求时，默认放行同一会话中的响应。请注意，会话保持的最长时间是910秒（s）。**

安全组类型

安全组分为普通安全组以及企业安全组，下表列举了两种类型安全组的差异。

安全组类型	安全组规则类型	安全组规则优先级	入方向访问策略	出方向访问策略	适用场景
普通安全组	默认安全组规则	由安全组模板决定 *	由安全组模板决定 *	允许所有访问请求	对网络精细化控制要求较高、希望使用多种ECS实例规格、以及网络连接数适中的用户场景
	自定义安全组规则	在1~100之间自定义一个数值	支持允许和拒绝策略，可按需添加 **	按需添加 **	
企业安全组	默认安全组规则	1，并且不支持修改	由安全组模板决定 *	由安全组模板决定 *	对运维效率、ECS实例规格以及计算节点的规模有更高需求的用户场景
	自定义安全组规则		支持允许策略，可按需添加 **	按需添加 **	

* 在ECS控制台上创建安全组时，您可以选择Web Server Linux（放行了80、443、22及ICMP协议）、Web Server Windows（放行了80、443、3389及ICMP协议）以及自定义（入方向上拒绝所有访问请求）的安全组模板。

** 自定义安全组规则的添加方法请参见添加安全组规则和安全组应用案例。

本文主要讲解普通安全组相关概念和使用方法，企业安全组请参见企业安全组概述。

默认安全组

在一个地域通过ECS管理控制台创建ECS实例时，如果当前账号在这个地域里尚未创建安全组，阿里云会为您创建的一个默认安全组，其类型为普通安全组。

默认安全组中的默认安全组规则如下：

- 入方向：放行了ICMP协议、SSH 22端口、RDP 3389端口，您还可以勾选放行HTTP 80端口和HTTPS 443端口。规则优先级为110。
- 出方向：允许所有访问。

规则优先级

手动添加安全组规则时，优先级范围为1到100，数值越小，优先级越高。默认安全组的规则优先级为110，表示该规则的优先级始终低于您手动添加的安全组规则。

ECS实例所在的安全组中，无论是同一个安全组内还是不同安全组之间，如果两条安全组规则的协议类型、端口范围、授权类型、授权对象都相同，最终生效的安全组规则如下：

- 如果优先级相同，则拒绝策略的授权规则优先生效，允许策略的授权规则不生效。
- 如果优先级不同，则优先级高的规则生效。

> **说明:**
> 企业安全组不支持规则优先级设置。

网络类型

普通安全组的网络类型不同时，安全组规则在网卡设置方面会有差异。

- 经典网络类型的安全组规则区分内网网卡和公网网卡。

- 专有网络VPC类型安全组规则不区分内网网卡和公网网卡。

  专有网络VPC类型ECS实例的公网访问通过内网网卡映射转发。所以，您在ECS实例内部无法看到公网网卡，也只能设置内网安全组规则，但安全组规则同时对内网和公网生效。

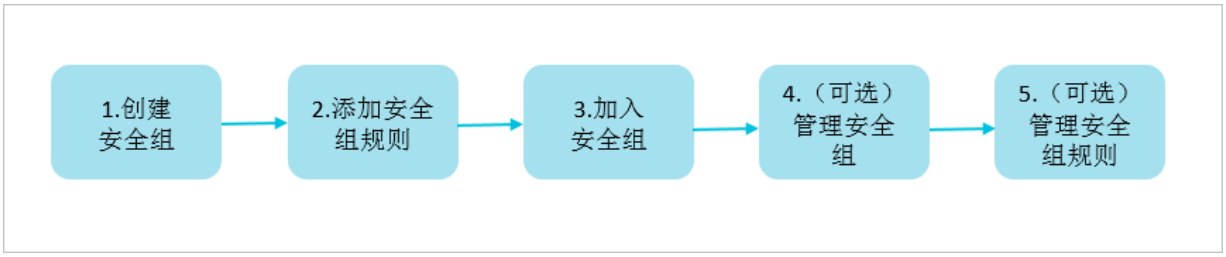
> **说明:**
> 企业安全组仅支持专有网络VPC。

使用限制

有关安全组的使用限制及配额，请参见*#unique_10*安全组章节。

使用流程

普通安全组的使用流程如下图所示，企业安全组的使用流程请参见企业安全组概述。



实践建议

以下为使用安全组时的实践建议：

- 您可以将安全组作为白名单使用，先设置为全部拒绝，然后逐一放行允许通信的访问请求策略。
- 为应用添加安全组规则时遵循最小授权原则。例如，您可以：
  - 选择开放具体的端口，不要设置为端口范围，如80/80端口。
  - 添加安全组规则时，谨慎授权0.0.0.0/0（全网段）访问源。
- 不建议使用一个安全组管理所有应用，不同的分层一定有不同的隔离需求。
- 不建议为每台ECS实例单独设置一个安全组，您只需将具有相同安全保护需求的ECS实例加入同一安全组即可。
- 建议您设置简洁的安全组规则。例如，如果您给一台ECS实例分配了多个安全组，该ECS实例很可能会同时遵循数百条安全组规则，任何规则变更都可能引起网络不通的故障。
- 如果您需要修改生产环境的安全组规则时，建议您使用克隆安全组功能。通过在克隆的安全组上进行调试，避免影响线上应用。关于如何克隆安全组，请参见克隆安全组。

1.2 企业安全组概述

企业级安全组拥有更高的ECS实例和弹性网卡数量容纳能力，以及无限制的私网IP地址管理能力，统一采用专有网络VPC，同时简化了安全组规则设置策略，更便于使用。企业级安全组适用于对运维效率、ECS实例规格以及计算节点规模有更高需求的场景。

功能对比

由于ECS实例以及弹性网卡不能同时加入普通安全组和企业安全组，建议您了解两种类型安全组的功能区别，并自行规划网络环境。更多有关普通安全组的详情，请参见安全组概述。

功能对比	普通安全组	企业安全组
是否支持所有实例规格	是	否，实例规格必须同时支持IPv6功能
是否支持专有网络VPC	是	是
是否支持经典网络	是	否
是否支持设置规则优先级	是	否
是否支持授权给其他安全组	是	否
是否支持手动设置允许访问的安全组规则	是	是
是否支持手动设置拒绝访问的安全组规则	是	否，企业安全组默认拒绝任何访问请求
支持的弹性网卡数量	受安全组内ECS实例数量限制	50000
是否支持绑定弹性网卡到任意实例规格	是，但实例网络类型必须是专有网络VPC	否，实例规格必须同时支持IPv6功能
能容纳的私网IP地址数量	2000	无限量

使用限制

有关企业安全组的使用限制及配额，请参见*#unique_10*安全组章节。

- 2019年5月30日之前创建的ECS实例不可以加入企业安全组。
- 实例规格必须同时支持IPv6功能时，才可以使用企业安全组。更多详情，请参见*#unique_12*。
- ECS实例和弹性网卡对所属的安全组类型有以下要求：
  - 一台ECS实例不能同时加入普通安全组和企业安全组。
  - 一张弹性网卡不能同时加入普通安全组和企业安全组。
  - 弹性网卡绑定到ECS实例时，两者的所属安全组类型必须相同。

控制台操作

在ECS管理控制台上，您可以按以下流程使用企业安全组。

1. 创建一个企业安全组，安全组类型选择为企业级安全组。详细步骤请参见创建安全组。
2. 添加一条允许访问的企业安全组规则。详细步骤请参见添加安全组规则。

   企业级安全组等同于通信白名单，只支持创建允许访问的规则，规则之间不存在优先级，授权对象只能是IP地址段不能是安全组。
3. 将一台支持IPv6功能的ECS实例加入到企业安全组，一台ECS实例不能同时加入普通和企业两种安全组。详细步骤请参见*ECS*实例加入安全组。
4. 在企业安全组中使用弹性网卡的步骤如下：

   a. 如果弹性网卡在普通安全组中，通过修改弹性网卡加入到企业安全组中。详细步骤请参见*#unique_15*。

   b. 将弹性网卡绑定到ECS实例。详细步骤请参见*#unique_16*。
5. （可选）管理企业安全组，如添加标签、修改名称与描述、管理企业安全组内的ECS实例等。详细步骤请参见：

   - 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

API操作

1. 调用*#unique_21*并将SecurityGroupType设置为enterprise。

   在创建安全组之前，您需要确保有可用的专有网络VPC与虚拟交换机。
2. 调用*#unique_22*添加一条入方向上允许访问的企业安全组规则，授权对象只能是IP地址段，不能是安全组。

   企业级安全组等同于白名单，策略（Policy）默认采用允许访问（accept）的规则，无需设置优先级（Priority）。您只需要指定通信协议（IpProtocol）、通信端口区间（PortRange）、（可选）源通信端口区间（SourcePortRange）、源IP地址段（SourceCidrIp）、（可选）目的端IP地址段（DestCiderIp）。
3. 调用*#unique_23*添加一条出方向上的企业安全组规则。
4. 调用*#unique_24*将专有网络VPC类型ECS实例入企业安全组。

5. 在企业安全组中使用弹性网卡的步骤如下：

   a. 如果弹性网卡在普通安全组中，调用*#unique_25*将弹性网卡加入到企业安全组。

   b. 调用*#unique_26*将已加入企业安全组的网卡挂载到ECS实例上。

6. （可选）调用*#unique_27*查看您在当前地域下已创建的安全组列表。

1.3 安全组应用案例

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**和**添加安全组规则**。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**

  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**

  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**

  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**

  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**

  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**

  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**

  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**

  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。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），您可以使用高速通道实现VPC互通。详情请参见*#unique_37*。

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	

- **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	

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			

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
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#unique_38。

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个账号的实例通过高速通道内网互通，再添加安全组规则。详情请参见#unique_39。

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			

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
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个账号的实例通过高速通道内网互通，再添加如下表所示的安全组规则。详情请参见*#unique_39*。

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			

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
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			

说明:

- 如果您无法通过http://公网IP地址访问您的实例，请参见检查*TCP 80*端口是否正常工作。
- 80端口是HTTP服务默认端口。如果要使用其他端口，如8080端口，您必须修改Web服务器配置文件中监听端口设置。

1.4 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*#unique_40*。
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。
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*#unique_41*。
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。

端口	服务	说明
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。

使用场景	网络类型	网卡类型	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	无需配置	入方向	允许	SSH(22)	22/22	地址段访问	0.0.0.0/0	1
	经典网络	公网							
RDP远程连接Windows实例	专有网络VPC	无需配置	入方向	允许	RDP(3389)	3389/3389	地址段访问	0.0.0.0/0	1
	经典网络	公网							
公网Ping ECS实例	专有网络VPC	无需配置	入方向	允许	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							
ECS实例作Web服务器	专有网络VPC	无需配置	入方向	允许	HTTP(80)	80/80	地址段访问	0.0.0.0/0	1
	经典网络	公网							
使用FTP上传或下载文件	专有网络VPC	无需配置	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							

1.5 创建安全组

安全组是ECS实例的虚拟防火墙。本文介绍如何在ECS控制台上创建一个安全组。

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和虚拟交换机。更多详情，请参见*#unique_42/unique_42_Connect_42_section_ufw_rhv_rdb*。

背景信息

每台ECS实例必须至少属于一个安全组。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仅设置针对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。更多详情，请参见安全组概述。如果您不希望ECS实例加入默认安全组，您可以根据本文描述，自行创建安全组。

操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 单击创建安全组。
5. 在弹出的创建安全组对话框中，完成以下配置。
   - 模板：根据安全组中的ECS实例需要部署的服务，选择合适的模板，简化安全组规则配置，如下表所示。

模板	说明	场景
Web Server Linux	默认放行TCP 80、TCP 443、TCP 22和ICMP协议入方向访问	安全组中的Linux实例上需要部署Web服务
Web Server Windows	默认放行TCP 80、TCP 443、TCP 3389和ICMP协议入方向访问	安全组中的Windows实例上需要部署Web服务
自定义	安全组创建成功后，按需自行添加安全组规则。具体操作，请参见添加安全组规则。	没有特殊需求

   - 安全组名称：按页面提示要求设置安全组名称。
   - 描述：简短地描述安全组，方便后期管理。
   - 安全组类型：
     - 普通安全组：适用于对网络精细化控制要求较高、希望使用多种ECS实例规格、以及网络连接数适中的用户场景。更多详情，请参见安全组概述。
     - 企业级安全组：适用于对运维效率、ECS实例规格以及计算节点的规模有更高需求的用户场景。更多详情，请参见企业安全组概述。

说明：

一台ECS实例不能同时加入普通安全组和企业安全组。

- **网络类型：**
  - **如果为经典网络类型安全组，选择经典网络。**
  - **如果为专有网络类型安全组，选择专有网络，并选择已经创建的专有网络VPC。**

> **说明：**
> **企业安全组仅支持专有网络VPC。**

6. 单击确定。

预期结果

创建成功后，安全组列表中新增了一个安全组。如果您在创建安全组时选择的是自定义模板，建议您根据页面提示设置安全组规则。

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。

相关文档
#unique_21

1.6 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，请确认以下信息：

- 您已经创建了一个安全组。具体操作，请参见创建安全组。
- 您已经知道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。

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，或者在创建安全组时选择了Web Server Linux模板或者Web Server Windows模板，则系统会给部分通信端口自动添加安全组规则，更多详情，请参见安全组概述。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：

- 安全组规则在网卡设置方面会有差异。
  - 经典网络类型的安全组规则区分内网网卡和公网网卡。
  - 专有网络VPC类型安全组规则不区分内网网卡和公网网卡。

    专有网络VPC类型ECS实例的公网访问通过内网网卡映射转发。所以，您在ECS实例内部无法看到公网网卡，也只能设置内网安全组规则，但安全组规则同时对内网和公网生效。
- 您自行创建的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。
- 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。
- 企业安全组不支持设置优先级、不支持授权给安全组、不支持设置拒绝访问的安全组规则。更多详情，请参见企业安全组概述。

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. 在顶部状态栏左上角处，选择地域。
4. 找到要配置授权规则的安全组，在操作列中，单击配置规则。
5. 在安全组规则页面上，您可以选择以下任意一种方式完成操作。
   - 方式一：快速创建规则，适用于无需设置ICMP、GRE协议规则，并通过勾选多个端口便能完成操作的场景。快速创建规则提供了SSH 22、telnet 23、HTTP 80、HTTPS 443、MS

SQL 1433、Oracle 1521、MySQL 3306、RDP 3389、PostgreSQL 5432和Redis 6379的应用端口设置。您可以同时勾选一个或多个端口，或者自定义TCP/UDP端口。

单击快速创建规则，快速创建规则对话框中的网卡类型、规则方向和端口范围等参数设置的详细指导请参见方式二添加安全组规则。

- 方式二：添加安全组规则，适用于需要设置多种通信协议的场景，如ICMP和GRE协议。

  a. 单击添加安全组规则。

  b. （仅经典网络类型安全组）选择网卡类型。

  - 内网：您的ECS实例不能访问公网/互联网，或者不需要访问公网。
  - 公网：您的ECS实例可以访问公网，并提供的是互联网访问应用。

  c. 选择规则方向。

  - 出方向：是指ECS实例访问内网中其他ECS实例或者公网上的资源。
  - 入方向：是指内网中的其他ECS实例或公网上的资源访问ECS实例。

  d. 选择授权策略。

  - 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。

  e. 选择协议类型和端口范围。

  端口范围的设置受协议类型影响，下表是创建页面中涉及的协议类型与端口范围的关系。更多常用端口信息，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。不能设置。	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。不能设置。	使用`ping`程序检测ECS实例之间的通信状况。
全部 ICMP（IPv6）	-1/-1，表示不限制端口。不能设置。	使用`ping6`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。不能设置。	用于VPN服务。

协议类型	端口显示范围	应用场景
自定义 TCP 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。
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#unique_38。
TELNET	23/23	用于Telnet远程登录ECS实例。
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。
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。
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#unique_38。
PostgreSQL	5432/5432	ECS实例作为PostgreSQL服务器。
Redis	6379/6379	ECS实例作为Redis服务器。

 **说明:**

公网出方向的STMP端口25默认受限，无法通过安全组规则打开。如果您需要使用STMP 25端口，请自行规避安全风险，然后申请解封端口25。具体操作，请参见申请解封端口25。

f. 选择授权类型和授权对象。

授权对象的设置受授权类型影响，以下是两者之间的关系。

授权类型	授权对象
IPv4 地址段访问	- 填写单一IP地址或者CIDR网段格式，如：12.1.1.1 或 13.1.1.1/25。 - 支持多组授权对象，用,隔开，最多支持10组授权对象。 - 如果填写0.0.0.0/0表示允许或拒绝所有IP地址的访问，设置时请务必谨慎。 关于CIDR格式介绍，请参见#unique_43。
IPv6 地址段访问	- 填写单一IP地址或者CIDR网段格式，如2001:0db8::1428:****或2001:0db8::1428:****/128。 - 支持多组授权对象，用,隔开，最多支持10组授权对象。 - 如果填写:: / 0表示允许或拒绝所有IP地址的访问，设置时请务必谨慎。
安全组访问	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实例访问本安全组中的ECS实例，实现内网互通。设置公网访问只能通过地址段访问授权。 - 本账号授权：选择同一账号下的其他安全组ID。如果是专有网络VPC类型的安全组，目的端必须为同一个专有网络VPC中的安全组。 - 跨账号授权：填写目标安全组ID，以及对方账号ID。在账号管理 > 安全设置里查看账号ID。 说明: 企业安全组不支持授权安全组访问。

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，则只能授权单个IP地址，授权对象的格式只能是a.b.c.d/32，仅支持IPv4，子网掩码必须是/32。

g. 优先级：取值范围为1~100。

> **说明:**
> 优先级数值越小，优先级越高。仅普通安全组可以设置优先级，企业安全组不支持设置优先级。更多详情，请参见规则优先级。

h. 单击确定。

预期结果

单击刷新图标查看已添加的安全组规则，确认已经完成添加。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。

后续步骤

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*。

相关文档
#unique_22
#unique_23

1.7 ECS实例加入安全组

您可以根据业务需要，将ECS实例加入一个或多个安全组。默认情况下，一台ECS实例可以加入五个安全组。

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*#unique_44*。
- 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，请参见安全组概述和企业安全组概述。

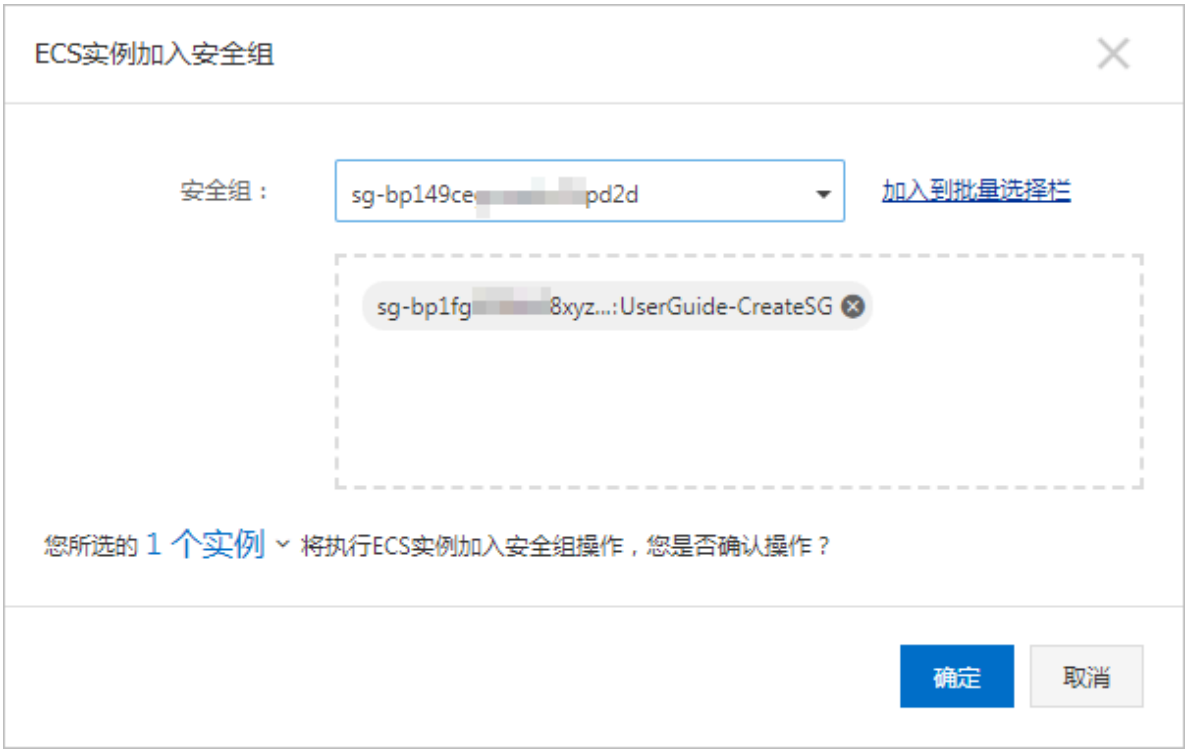
背景信息

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。一台ECS实例至少属于一个安全组，最多不能超过五个安全组。

在云服务器ECS管理控制台上通过实例页面将ECS实例加入安全组的操作路径如下，您也可以通过网络与安全 > 安全组的路径完成操作。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，单击实例与镜像 > 实例。
3. 在顶部状态栏左上角处，选择地域。
4. 在实例列表页面中，找到需要加入安全组的ECS实例，在操作列中，单击管理。
5. 在左侧导航栏，单击本实例安全组。
6. 单击加入安全组。
7. 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。



8. 单击确定。

加入安全组后，安全组规则对ECS实例自动生效。

后续步骤

- 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，请参见查询安全组列表。
- 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
#unique_24

1.8 管理安全组规则

1.8.1 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，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，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
#unique_47

1.8.2 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。您可以查看潜在高危安全组发现不合理的安全组规则，通过修改安全组规则保证ECS实例的网络安全。具体操作，请参见查看潜在高危安全组概览。

操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，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，单击操作列下的修改。
   - 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。

1.8.3 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。

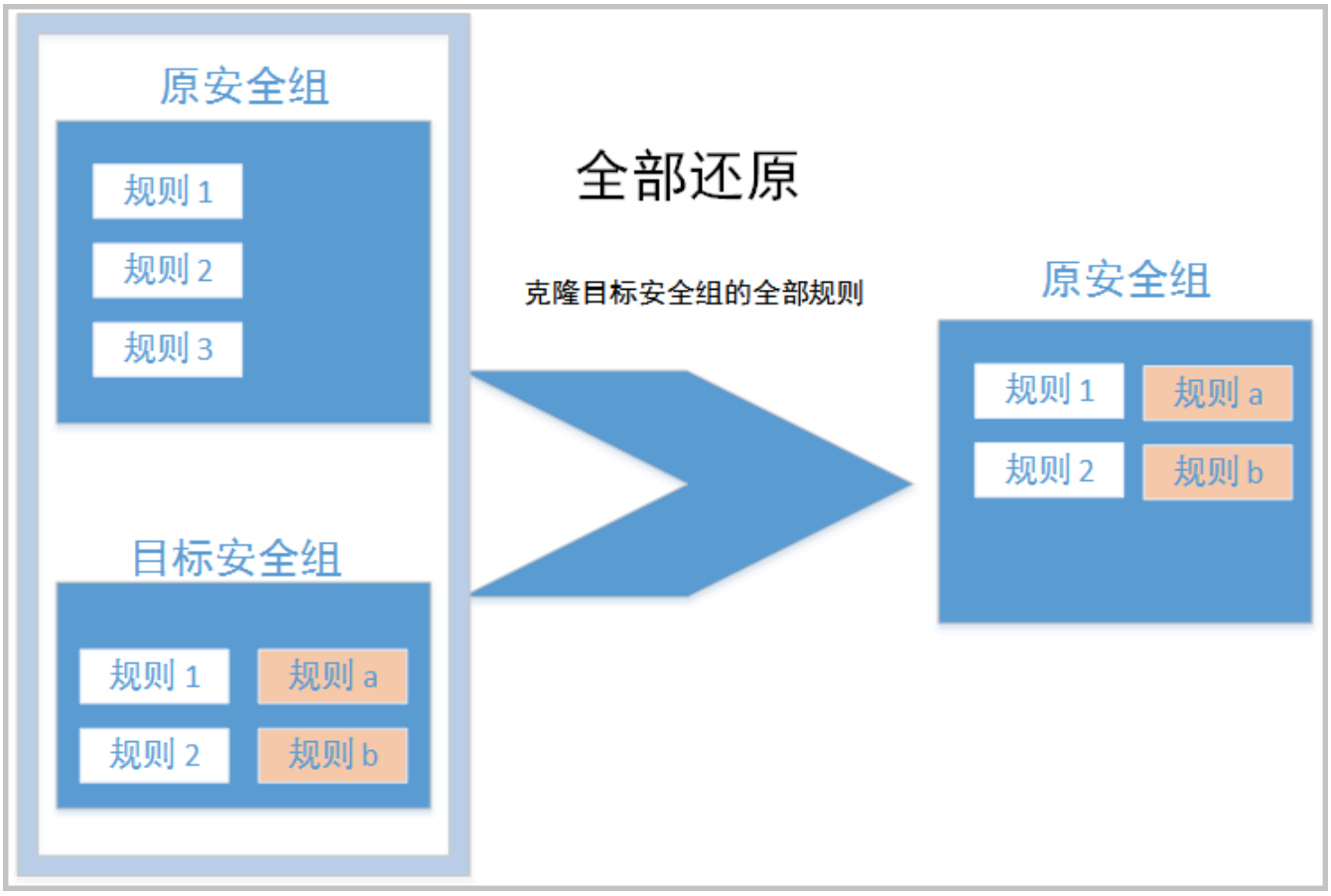
前提条件

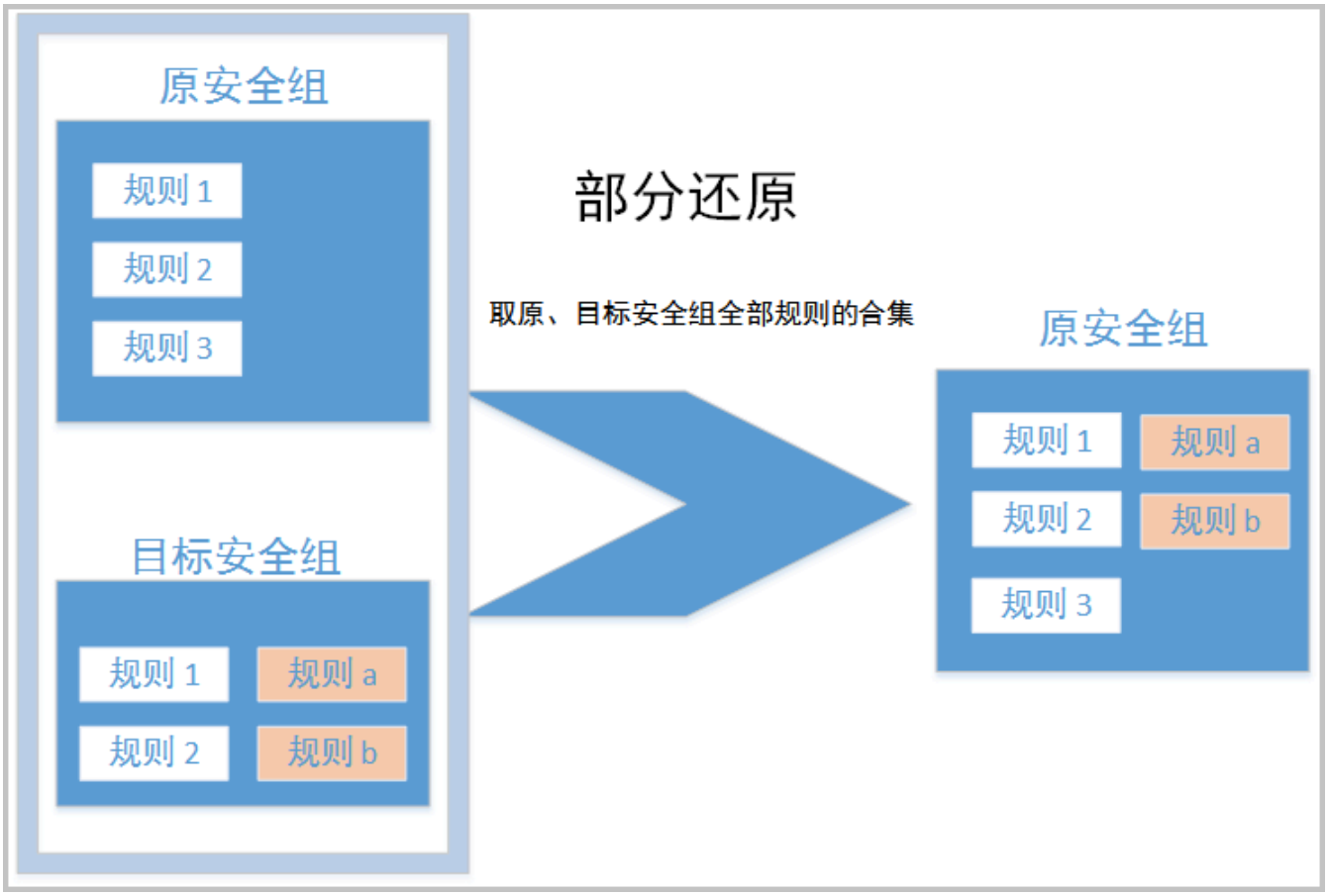
- 原安全组与目标安全组必须在同一个地域。
- 原安全组与目标安全组必须为同一种网络类型。

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。


原安全组
规则 1
规则 2
规则 3
目标安全组
规则 1
规则 a
规则 2
规则 b
全部还原
克隆目标安全组的全部规则
原安全组
规则 1
规则 a
规则 2
规则 b


原安全组
规则 1
规则 2
规则 3
目标安全组
规则 1
规则 a
规则 2
规则 b
部分还原
取原、目标安全组全部规则的合集
原安全组
规则 1
规则 a
规则 2
规则 b
规则 3

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，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，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。

   a) 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。

   b) 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。

   c) 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。

   d) 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。

预期结果

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。

1.8.4 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，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，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，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. 单击导出全部规则，下载并保存JSON文件到本地。

   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*。

1.8.5 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。

操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，找到需要导入安全组规则的安全组，单击操作列下的配置规则。
5. 单击导入规则。
6. 选择要导入的JSON文件，将会生成预览规则。

   预览规则显示以下信息：

   - 导入的规则数。
   - 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。
8. 查看导入安全组规则的结果，单击导入结束，关闭。

1.8.6 删除安全组规则

如果您不再需要某个安全组规则，可以删除安全组规则。

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。
- 请确认您的ECS实例不需要允许/禁止哪些公网访问或内网访问。

操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，找到需要删除规则的安全组，单击操作列下的配置规则。
5. 单击安全组规则所属的方向。
   - 如果您需要删除专有网络类型的安全组规则，请选择入方向或出方向。
   - 如果您需要删除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. 找到需要删除的安全组规则，单击操作列下的删除。
7. 在弹出的删除安全组规则对话框中，阅读提示信息，确认无误后，单击确定。

相关文档
#unique_55
#unique_56

1.9 管理安全组

1.9.1 查询安全组

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。

操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，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搜索，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并单击搜索，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并单击搜索，可查询到该专有网络下的所有安全组。

1.9.2 修改安全组

如果您想修改安全组的名称和描述信息，您可以修改安全组属性。

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。

操作步骤

1. 登录ECS管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，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。

相关文档
#unique_58

1.9.3 克隆安全组

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

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*#unique_59*。

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，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。

4. 在安全组列表页面中，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。
6. 单击确定。

预期结果

创建成功后，克隆对话框会自动关闭。您可以在安全组列表里看到克隆出来的新安全组。

1.9.4 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。

操作步骤

1. 登录*ECS管理控制台*。
2. 在左侧导航栏，单击实例与镜像 > 实例。
3. 在顶部状态栏左上角处，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. 单击本实例安全组。
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。

相关文档

#unique_60

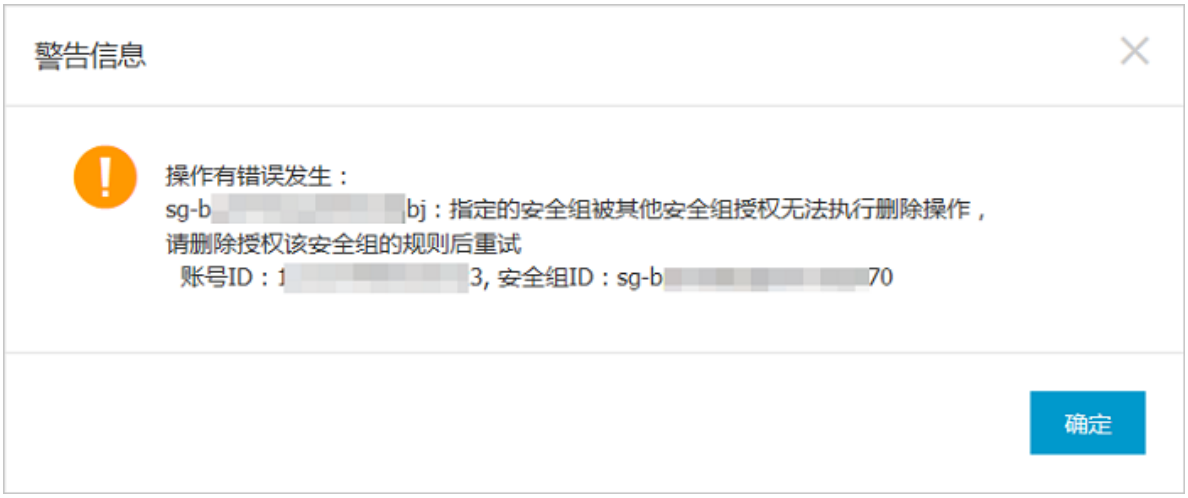
1.9.5 删除安全组

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。

- 安全组与其他安全组之间没有授权行为。您可以按本文描述的步骤直接删除安全组，如果该安全组被其他安全组授权，您将看到如下图所示的错误信息，您可以删除相应的授权规则。



操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏，单击网络与安全 > 安全组。
3. 在顶部状态栏左上角处，选择地域。
4. 在安全组列表页面中，选中一个或多个安全组，在列表底部，单击删除。
5. 在删除安全组对话框里，确认信息后，单击确定。

相关文档

#unique_61

2 SSH密钥对

2.1 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。**

- 一台Linux实例只能绑定一个SSH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。
- 已停售的实例规格无法使用SSH密钥对。详情请参见#unique_64。
- 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。详情请参见#unique_65。

  说明：

  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下列任一种加密方式：
  - 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 账号访问控制

本文介绍了如何使用访问控制RAM（Resource Access Management）在账号级别上控制对云服务器ECS资源的访问，具体通过创建RAM用户（组）并授予特定权限策略实现。

背景信息

访问控制RAM是阿里云提供的资源访问控制服务。更多详情，请参见*#unique_67*。以下列举了访问控制RAM的典型场景：

- 用户：如果您购买了多台云服务器ECS实例，您的组织里有多个用户（如员工、系统或应用程序）需要使用这些实例，您可以创建一个策略允许部分用户使用这些实例。避免了将同一个AccessKey泄露给多人的风险。
- 用户组：您可以创建多个用户组，并授予不同权限策略，起到批量管理的效果。例如：
  - 为了加强网络安全控制，您可以给某个用户组授权一个权限策略，该策略可以规定：如果用户的IP地址不是来自企业网络，则拒绝此类用户请求访问相关ECS资源。
  - 您可以创建以下两个用户组管理不同工作职责的人员，如果某开发人员的工作职责发生转变，成为一名系统管理人员，您可以将其从Developpers用户组移到SysAdmins用户组。
    - SysAdmins：该用户组需要创建和管理的权限。您可以给SysAdmins组授予一个权限策略，该策略授予用户组成员执行所有ECS操作的权限，包括ECS实例、镜像、快照和安全组等。
    - Developers：该用户组需要使用实例的权限。您可以给Developers组授予一个权限策略，该策略授予用户组成员调用DescribeInstances、StartInstance、StopInstance、RunInstance和DeleteInstance等权限。

权限策略

权限策略分为系统策略和自定义策略。

- 系统策略：阿里云提供多种具有不同管理目的的默认权限策略。云服务器ECS经常使用的系统策略有：
  - AliyunECSReadOnlyAccess：只读访问云服务器ECS的权限。
  - AliyunECSFullAccess：云服务器ECS的管理员级别权限。
  - AliyunECSImageImportDefaultRole：导入自定义镜像的权限。
  - AliyunECSImageExportDefaultRole：导出自定义镜像的权限。
  - AliyunECSNetworkInterfaceManagementAccess：管理弹性网卡的权限。

- **自定义策略：需要您精准地设计权限策略，适用于熟悉阿里云各种云服务API以及具有精细化控制需求的用户。如下文（可选）创建自定义权限策略步骤中创建的自定义策略。**

前提条件

您已使用云账号登录*RAM*控制台。

操作步骤

本文示例使用主账号在RAM控制台创建一个RAM用户，并授予自定义权限或者系统权限：

1. **创建*RAM*用户**
2. **（可选）创建自定义权限策略**
3. **授权*RAM*用户**

创建RAM用户

按以下步骤在访问控制RAM控制台创建一个RAM用户：

1. **在左侧导航栏的人员管理菜单下，单击用户。**
2. **单击新建用户。**

   说明：
   单击添加用户，可一次性创建多个RAM用户。

3. **输入登录名称和显示名称。**
4. **在访问方式区域下，选择控制台密码登录或编程访问。**

   说明：
   为了保障账号安全，建议仅为RAM用户选择一种登录方式，避免RAM用户离开组织后仍可以通过访问密钥访问阿里云资源。

5. **单击确认。**

（可选）创建自定义权限策略

除了使用阿里云提供的系统权限，您还可以按以下步骤在访问控制RAM控制台创建一个自定义权限策略：

1. **在左侧导航栏的权限管理菜单下，单击权限策略管理。**
2. **单击新建权限策略。**
3. **填写策略名称和备注。**

4. 配置模式选择可视化配置或脚本配置。

   - 可视化配置：单击添加授权语句，根据界面提示，对权限效力、操作名称和资源等进行配置。
   - 脚本配置：请参考*#unique_71*编辑策略内容。

   选择脚本配置时，Statement结构下的Action和Resource参数取值请参见**鉴权列表**，其他参数取值请参见《访问控制文档》*#unique_71*。

   - 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实例后查询实例和磁盘信息。**

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

5. **单击确定。**

授权RAM用户

按以下步骤在访问控制RAM控制台创授权RAM用户相关权限：

1. **在左侧导航栏的人员管理菜单下，单击用户。**
2. **在用户登录名称/显示名称列表下，找到目标RAM用户。**
3. **单击添加权限，被授权主体会自动填入。**
4. **在左侧权限策略名称列表下，单击需要授予RAM用户的权限策略。**

> **说明:**
> **在右侧区域框，选择某条策略并单击×，可撤销该策略。**

5. **单击确定。**
6. **单击完成。**

后续步骤

完成授权后，权限立即生效，RAM用户可以登录*RAM*控制台操作目标云资源。

4 实例RAM角色

4.1 实例RAM角色概述

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。

背景信息

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（临时凭证将周期性更新）访问其他云产品的API。一方面可以保证AccessKey安全，另一方面也可以借助RAM实现权限的精细化控制和管理。关于角色的详细描述，请参见角色。

一般情况下，ECS实例的应用程序是通过用户账号或者RAM用户的AccessKey访问阿里云各产品的API。详情请参见*RAM*用户。

为了满足调用需求，需要直接把AccessKey固化在实例中，如写在配置文件中。但是这种方式权限过高，存在泄露信息和难以维护等问题。因此，阿里云推出了实例RAM角色解决这些问题。

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。**
- **安全地在ECS实例中使用STS临时凭证访问阿里云的其他云服务，例如OSS、ECS、RDS等。**
- **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。**

费用详情

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：

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

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。

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。参见RAM文档开通方法。
- 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。详细步骤请参见授权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。详细步骤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. 步骤三：授予实例RAM角色
3. 步骤二：授权实例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. 云账号登录RAM控制台。
2. 在左侧导航栏，单击RAM角色管理。
3. 单击新建RAM角色，选择可信实体类型为阿里云服务，单击下一步。
4. 输入角色名称和备注。
5. 选择受信服务为云服务器。
6. 单击完成。

步骤二：授权实例RAM角色

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. **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，单击RAM角色管理。**
4. **在RAM角色名称列表下，单击目标RAM角色名称。**
5. **在权限管理页签下，单击精确授权。**
6. **选择权限类型为系统策略或自定义策略。**
7. **输入策略名称。**
8. **单击确定。**
9. **单击关闭。**

步骤三：授予实例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，单击实例与镜像 > 实例。**
3. **在顶部状态栏左上角处，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RAM角色属性中为实例选择已创建好的实例RAM角色。更多详情请参见*#unique_44*。

相关文档

#unique_83

#unique_84

#unique_85

#unique_86

4.3 管理实例RAM角色

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，单击实例与镜像 > 实例。
3. 在顶部状态栏左上角处，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
#unique_86

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，单击实例与镜像 > 实例。

3. 在顶部状态栏左上角处，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

#unique_90

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*#unique_91*。

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：执行命令`curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting`。
   - Windows实例：执行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" : "XXXXXXXXX",
   "AccessKeySecret" : "XXXXXXXXX",
   "Expiration" : "2017-11-01T05:20:01Z",
   "SecurityToken" : "XXXXXXXXX",
   "LastUpdated" : "2017-10-31T23:20:01Z",
   "Code" : "Success"
}
```

相关文档
#unique_92

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. 云账号登录*RAM*控制台。
2. 在左侧导航栏的人员管理菜单下，单击用户。
3. 在用户登录名称/显示名称列表下，找到目标RAM用户。
4. 在左侧权限策略名称列表下，单击需要授予RAM用户的权限策略。

   授权策略如下所示，其中，`[ECS RAM Action]`表示可授权RAM用户的权限，更多取值请参见*#unique_72*。

```
{
        "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": "*"
            }
        ]
}
```

说明:

在右侧区域框，选择某条策略并单击×，可撤销该策略。

5. **单击确定。**
6. **单击完成。**

相关文档

#unique_84

#unique_85

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，详情请参见RAM文档*#unique_80*。

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。详情请参见获取临时授权*Token*。**
- **如果您是通过RAM用户子账号使用实例RAM角色，您需要通过云账号授权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。

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

步骤二：授权实例RAM角色

完成以下操作，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*DettachInstanceRamRole*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

完成以下操作，创建实例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*#unique_101*。

```
{
        "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，详情请参见*#unique_72*。

相关文档

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。

#unique_78

#unique_83

#unique_102

#unique_84

#unique_85

#unique_86

#unique_90

#unique_103

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恶意流量攻击，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，详情请参见*#unique_105*。

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。更详细的信息，请参见*DDoS基础防护服务-产品架构*。

> **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。详细信息，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。

云服务器ECS的清洗阈值

云服务器ECS的清洗阈值由实例规格决定。下表列出了目前在售和已停售的部分实例规格的清洗阈值。详情请参见*在售的实例规格*和*#unique_64*。

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.g5.16xlarge	20000	4000000

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.g5.22xlarge	30000	4500000
ecs.g5.2xlarge	2500	800000
ecs.g5.4xlarge	5000	1000000
ecs.g5.6xlarge	7500	1500000
ecs.g5.8xlarge	10000	2000000
ecs.g5.large	1000	300000
ecs.g5.xlarge	1500	500000
ecs.sn2ne.14xlarge	10000	4500000
ecs.sn2ne.2xlarge	2000	1000000
ecs.sn2ne.4xlarge	3000	1600000
ecs.sn2ne.8xlarge	6000	2500000
ecs.sn2ne.large	1000	300000
ecs.sn2ne.xlarge	1500	500000
ecs.c5.16xlarge	20000	4000000
ecs.c5.2xlarge	2500	800000
ecs.c5.4xlarge	5000	1000000
ecs.c5.6xlarge	7500	1500000
ecs.c5.8xlarge	10000	2000000
ecs.c5.large	1000	300000
ecs.c5.xlarge	1500	500000
ecs.sn1ne.2xlarge	2000	1000000
ecs.sn1ne.4xlarge	3000	1600000
ecs.sn1ne.8xlarge	6000	2500000
ecs.sn1ne.large	1000	300000
ecs.sn1ne.xlarge	1500	500000
ecs.r5.16xlarge	20000	4000000
ecs.r5.22xlarge	30000	4500000
ecs.r5.2xlarge	2500	800000
ecs.r5.4xlarge	5000	1000000
ecs.r5.6xlarge	7500	1500000

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.r5.8xlarge	10000	2000000
ecs.r5.large	1000	300000
ecs.r5.xlarge	1500	500000
ecs.re4.20xlarge	15000	2000000
ecs.re4.40xlarge	30000	4000000
ecs.se1ne.14xlarge	10000	4500000
ecs.se1ne.2xlarge	2000	1000000
ecs.se1ne.4xlarge	3000	1600000
ecs.se1ne.8xlarge	6000	2500000
ecs.se1ne.large	1000	300000
ecs.se1ne.xlarge	1500	500000
ecs.se1.14xlarge	10000	1200000
ecs.se1.2xlarge	1500	400000
ecs.se1.4xlarge	3000	500000
ecs.se1.8xlarge	6000	800000
ecs.se1.large	500	100000
ecs.d1ne.2xlarge	6000	1000000
ecs.d1ne.4xlarge	12000	1600000
ecs.d1ne.6xlarge	16000	2000000
ecs.d1ne.8xlarge	20000	2500000
ecs.d1ne.14xlarge	35000	4500000
ecs.d1.2xlarge	3000	300000
ecs.d1.4xlarge	6000	600000
ecs.d1.6xlarge	8000	800000
ecs.d1.8xlarge	10000	1000000
ecs.d1-c8d3.8xlarge	10000	1000000
ecs.d1.14xlarge	17000	1800000
ecs.d1-c14d3.14xlarge	17000	1400000
ecs.i2.xlarge	1000	500000
ecs.i2.2xlarge	2000	1000000

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.i2.4xlarge	3000	1500000
ecs.i2.8xlarge	6000	2000000
ecs.i2.16xlarge	10000	4000000
ecs.i1.xlarge	800	200000
ecs.i1.2xlarge	1500	400000
ecs.i1.4xlarge	3000	500000
ecs.i1-c10d1.8xlarge	6000	800000
ecs.i1-c5d1.4xlarge	3000	400000
ecs.i1.14xlarge	10000	1200000
ecs.hfc5.large	1000	300000
ecs.hfc5.xlarge	1500	500000
ecs.hfc5.2xlarge	2000	1000000
ecs.hfc5.4xlarge	3000	1600000
ecs.hfc5.6xlarge	4500	2000000
ecs.hfc5.8xlarge	6000	2500000
ecs.hfg5.large	1000	300000
ecs.hfg5.xlarge	1500	500000
ecs.hfg5.2xlarge	2000	1000000
ecs.hfg5.4xlarge	3000	1600000
ecs.hfg5.6xlarge	4500	2000000
ecs.hfg5.8xlarge	6000	2500000
ecs.hfg5.14xlarge	10000	4000000
ecs.c4.2xlarge	3000	400000
ecs.c4.4xlarge	6000	800000
ecs.c4.xlarge	1500	200000
ecs.ce4.xlarge	1500	200000
ecs.cm4.4xlarge	6000	800000
ecs.cm4.6xlarge	10000	1200000
ecs.cm4.xlarge	1500	200000
ecs.gn5-c28g1.14xlarge	10000	4500000

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.gn5-c4g1.xlarge	3000	300000
ecs.gn5-c4g1.2xlarge	5000	1000000
ecs.gn5-c8g1.2xlarge	3000	400000
ecs.gn5-c8g1.4xlarge	5000	1000000
ecs.gn5-c28g1.7xlarge	5000	2250000
ecs.gn5-c8g1.8xlarge	10000	2000000
ecs.gn5-c8g1.14xlarge	25000	4000000
ecs.gn5i-c2g1.large	1000	100000
ecs.gn5i-c4g1.xlarge	1500	200000
ecs.gn5i-c8g1.2xlarge	2000	400000
ecs.gn5i-c16g1.4xlarge	3000	800000
ecs.gn5i-c28g1.14xlarge	10000	2000000
ecs.gn4-c4g1.xlarge	3000	300000
ecs.gn4-c8g1.2xlarge	3000	400000
ecs.gn4-c4g1.2xlarge	5000	500000
ecs.gn4-c8g1.4xlarge	5000	500000
ecs.gn4.8xlarge	6000	800000
ecs.gn4.14xlarge	10000	1200000
ecs.ga1.xlarge	1000	200000
ecs.ga1.2xlarge	1500	300000
ecs.ga1.4xlarge	3000	500000
ecs.ga1.8xlarge	6000	800000
ecs.ga1.14xlarge	10000	1200000
ecs.f1-c28f1.7xlarge	5000	2000000
ecs.f1-c8f1.2xlarge	2000	800000
ecs.f2-c28f1.14xlarge	10000	2000000
ecs.f2-c28f1.7xlarge	5000	1000000
ecs.f2-c8f1.2xlarge	2000	400000
ecs.f2-c8f1.4xlarge	5000	1000000
ecs.t5-c1m1.2xlarge	1200	400000

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.t5-c1m1.large	500	100000
ecs.t5-c1m1.xlarge	800	200000
ecs.t5-c1m1.4xlarge	1200	600000
ecs.t5-c1m2.2xlarge	1200	400000
ecs.t5-c1m2.large	500	100000
ecs.t5-c1m2.xlarge	800	200000
ecs.t5-c1m2.4xlarge	1200	600000
ecs.t5-c1m4.2xlarge	1200	400000
ecs.t5-c1m4.large	500	100000
ecs.t5-c1m4.xlarge	800	200000
ecs.t5-lc1m1.small	200	60000
ecs.t5-lc1m2.large	400	100000
ecs.t5-lc1m2.small	200	60000
ecs.t5-lc1m4.large	400	100000
ecs.t5-lc2m1.nano	100	40000
ecs.ebmg4.8xlarge	10000	4500000
ecs.ebmg5.24xlarge	10000	4500000
ecs.sccg5.24xlarge	10000	4500000
ecs.xn4.small	500	50000
ecs.mn4.small	500	50000
ecs.mn4.large	500	100000
ecs.mn4.xlarge	800	150000
ecs.mn4.2xlarge	1200	300000
ecs.mn4.4xlarge	2500	400000
ecs.n4.small	500	50000
ecs.n4.large	500	100000
ecs.n4.xlarge	800	150000
ecs.n4.2xlarge	1200	300000
ecs.n4.4xlarge	2500	400000
ecs.n4.8xlarge	5000	500000

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.e4.small	500	50000
ecs.sn1.medium	500	100000
ecs.sn1.large	800	200000
ecs.sn1.xlarge	1500	400000
ecs.sn1.3xlarge	3000	500000
ecs.sn1.7xlarge	6000	800000
ecs.sn2.medium	500	100000
ecs.sn2.large	800	200000
ecs.sn2.xlarge	1500	400000
ecs.sn2.3xlarge	3000	500000
ecs.sn2.7xlarge	6000	800000
ecs.sn2.13xlarge	10000	120000

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5 Gbit/s时，您的ECS实例会被打进黑洞。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，主要提供免费版的安全预防和入侵检测服务。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。更多详情，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》*#unique_112*。

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*#unique_113*。

您可以按以下方式操作Agent。

- 创建ECS实例时自动安装Agent

  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. 在顶部状态栏处，选择地域。
  4. 创建一台ECS实例，在镜像配置处，勾选安全加固，系统自动为新建ECS实例安装Agent。详情请参见#unique_44。

> 说明:
> 您也可以在调用#unique_114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

  1. 登录ECS管理控制台。
  2. 在概览页面，单击云安全中心前往云盾控制台。
  3. 安装Agent。具体操作，请参见《云安全中心文档》#unique_115。

- 卸载Agent

  1. 登录ECS管理控制台。
  2. 在概览页面，单击云安全中心前往云盾控制台。
  3. 卸载Agent。具体操作，请参见《云安全中心文档》#unique_116。

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，单击实例与镜像 > 实例。
3. 在顶部状态栏左上角处，选择地域。

4. 按以下任一方式查看安全状态：

   - 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，单击云安全中心前往云盾控制台。
3. 在左侧导航栏，单击设置，并切换到通知页面。
4. 在安全告警项目处，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》*#unique_117*查看更多告警方式。

相关文档

云安全中心基础版、高级版和企业版功能对比

#unique_119

#unique_120

#unique_114

7 安全FAQ

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。同一安全组内的ECS实例之间网络互通，不同安全组的ECS实例之间默认内网不通，可以授权两个安全组之间互访。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。详情请参见安全组默认规则。

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x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。

为什么专有网络VPC类型ECS实例不能设置公网安全组规则?

专有网络VPC类型ECS实例的公网访问通过内网网卡映射完成，您在ECS实例内部看不到公网网卡，在安全组里只能设置内网规则。您设置的安全组规则同时对内网和公网生效。

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。具体设置，请参见使用SSL加密465端口发信样例及Demo。如果您只能使用TCP 25端口，请申请解封。具体操作，请参见TCP 25端口控制台解封申请。更多应用，请参见安全组应用案例。

为什么无法访问80端口?

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，请参见数据管理DMS登录云服务器的IP是什么。**

- 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。

为什么有的安全组规则的优先级是110?

优先级为110的安全组规则是由系统创建的默认安全组规则，表示默认规则的优先级永远比您手动添加的安全组规则低。手动添加安全组规则时，优先级只能设置为1~100。

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。比如：

- 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*#unique_10*。

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。

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*#unique_10*。