阿里云
云服务器 ECS

安全

文档版本：20190409

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
	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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 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。	`swich` *`{stand | slave}`*

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，可以配置一系列的安全组规则，允许或禁止安全组内的ECS实例对公网或私网的访问。安全组是重要的网络安全隔离手段，用于在云端划分安全域。

安全组分类

安全组由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。在创建实例时需要指定安全组，每个实例至少属于一个安全组。同一安全组内的实例之间默认内网网络互通，不同安全组的实例之间默认内网不通。可以通过安全组规则授权两个安全组之间互访。

安全组有两种类型，如下表所示：

安全组类型	安全组规则类型	安全组规则优先级	入方向规则	出方向规则	适用场景
默认安全组	默认安全组的默认规则。	110	放行 ICMP 协议、SSH 22 端口、RDP 3389 端口，禁止其他所有访问，您可以勾选放行 HTTP 80 和 HTTPS 443 端口。	允许所有访问。	同一VPC中没有自定义安全组。
自定义安全组	自定义安全组的默认规则。	110	拒绝所有访问。	允许所有访问。	同一VPC中已创建自定义安全组，但没有添加安全组规则。
	自定义安全组的自定义规则。	自定义，可设置1~100之间的任一个数值	按需添加安全组规则。详情请参见添加安全组规则和安全组应用案例。	按需添加的安全组规则。详情请参见添加安全组规则和安全组应用案例。	同一VPC中已创建自定义安全组，并且已添加安全组规则。

网络类型不同，安全组规则不同。

经典网络类型的安全组规则区分内网和公网，VPC 类型安全组规则不区分内网和公网。VPC 类型 ECS 实例的公网访问通过私网网卡映射完成，所以，您在实例内部看不到公网网卡，在安全组里也只能设置内网规则。安全组规则同时对内网和公网生效。

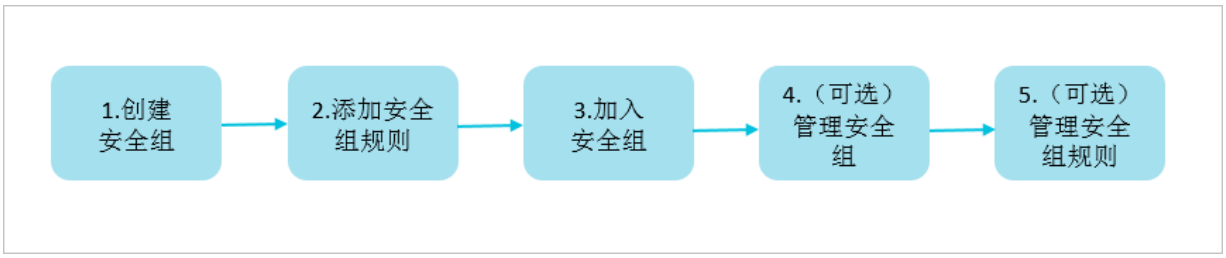
安全组优先级

安全组规则的优先级数值越小，优先级越高。

ECS实例可以加入不同的安全组。无论是同一个安全组内或不同安全组之间，如果安全组规则互相矛盾，即协议类型、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，则拒绝授权规则生效，允许授权规则不生效。
- 如果优先级不同，则优先级高的规则生效，与授权策略的设置无关。

使用流程



安全组实践建议

- 安全组作为白名单使用。
- 开放应用出入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（如 80 端口）。
- 不应使用一个安全组管理所有应用，不同的分层一定有不同的安全组需求。
- 将具有相同安全保护需求的实例加入同一安全组，无需为每个实例单独设置一个安全组。
- 设置简洁的安全组规则。如果您给一个实例分配多个安全组，则该实例可能会应用多达数百条规则。访问该实例时，可能会出现网络不通的问题。
- ECS控制台提供了克隆安全组和安全组规则的功能。如果您想要修改线上的安全组和规则，先克隆一个安全组，再在克隆的安全组上进行调试，从而避免直接影响线上应用。

1.2 安全组限制

本文介绍安全组及安全组规则的限制。

安全组限制

- 每个账号在每个地域最多可创建 100 个安全组，并可以根据您的会员等级的提高而增加。如需提高上限，请提交工单。

- 一个实例中的每个弹性网卡默认最多可以加入 5 个安全组。如需提高上限，请提交工单，阿里云会评估您的业务量是否需要更多的安全组，评估通过后可以增加到 10 个或者 16 个安全组。
- 安全组的网络类型分为经典网络和专有网络。
  - 经典网络类型的实例可以加入同一地域（Region）下经典网络类型的安全组。

    单个经典网络类型的安全组内的实例个数不能超过 1000。如果您有超过 1000 个实例需要内网互访，可以将他们分配到多个安全组内，并通过互相授权的方式允许互访。
  - 专有网络类型的实例可以加入同一专有网络（VPC）下的安全组。

    单个 VPC 类型的安全组内的私网 IP 个数不能超过 2000（主网卡和辅助网卡共享此配额）。如果您有超过 2000 个私网 IP 需要内网互访，可以将这些私网 IP 的实例分配到多个安全组内，并通过互相授权的方式允许互访。
- 如果数据包在 Outbound 方向是被允许的，那么对应的此连接在 Inbound 方向也是允许的。

更多信息，请参见安全组FAQ。

安全组规则的限制

每个弹性网卡的安全组规则数量上限 = 该实例可加入的安全组数量 x 每个安全组最大规则数量。一个实例中的每个弹性网卡最多可以设置 1000 条安全组规则。

- 默认情况下，一个弹性网卡最多加入 5 个安全组，每个安全组 200 个规则，即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。
- 每个安全组内规则数量会随网卡可加入安全组数量变化而变化，但总数不能超过 200，而且不会单独计算入站规则和出站规则。
  - 如果您调整到每个弹性网卡可加入 10 个安全组，那么每个安全组只允许 100 个规则。
  - 如果您调整到每个弹性网卡可加入 16 个安全组，那么每个安全组只允许 60 个规则。

安全组和安全组规则的数量的关系如下：

当安全组数量为	则安全组规则数量的上限为（入方向和出方向共享此配额）
5 个（默认值）	200 条
10 个（需提交工单）	100 条
16 个（需提交工单）	60 条

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。

说明:

- 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。
- 常用端口，请参见常用端口的典型应用。

- 案例 1#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 2#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 3#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 4#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 5#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 6#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 7#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 8#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。

案例 1：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 2 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。

案例 2：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 3：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，如1.2.3.4。	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，如1.2.3.4。	1
经典网络	公网							

案例 4：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，如1.2.3.4。	1
经典网络	公网							

添加了安全组规则后，在连接实例，执行 `ping`、`telnet` 等测试。如果实例只能访问允许访问的 IP 地址，说明安全组规则已经生效。

案例 5：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，如1.2.3.4。	1
经典网络	公网							

案例 6：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，参见案例2#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，如8080/8080			
经典网络	公网	入方向	允许	Windows：RDP(3389)	3389/3389	地址段访问	如果允许任意公网IP地址连接实例，填写0.0.0.0/0。如果只允许特定公网IP地址连接实例，参见案例2#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，如8080/8080			

自定义远程连接端口的详细操作，请参见服务器默认远程端口修改。

案例 7：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。

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，如8080/8080			
经典网络	内网	入方向	允许	Windows：RDP(3389)	3389/3389	地址段访问	对方实例的内网IP地址，出于安全性考虑，仅支持单IP授权，例如：a.b.c.d/32。	1
				Linux：SSH(22)	22/22			
				自定义TCP	自定义，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。

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，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	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，如8080/8080			

案例 8：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，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。	1
				HTTPS(443)	443/443			
				自定义TCP	自定义，如8080/8080			
经典网络	公网	入方向	允许	HTTP(80)	80/80	地址段访问	允许访问您网站的主机的公网IP地址，可以为一个或多个公网IP地址。	1
				HTTPS(443)	443/443			
				自定义TCP	自定义，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 常用端口的典型应用

如果您了解 ECS 实例的常用端口，您可以更准确的添加和修改安全组规则。本文为您介绍 ECS 实例常用端口及常用端口的典型应用。

常用端口列表

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使用用户名密码验证连接*Linux*实例。
23	Telnet	Telnet 端口，用于 Telnet 远程登录 ECS 实例。

端口	服务	说明
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。 您可以参见检查 *TCP 80* 端口是否正常工作 排查 80 端口故障。
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。
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

使用场景	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
SSH 远程连接 Linux 实例	VPC 网络	不需要配置	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	VPC 网络	不需要配置	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	VPC 网络	不需要配置	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	VPC 网络	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
	经典网络	公网							
使用 FTP 上传或下载文件	VPC 网络	不需要配置	入方向	允许	自定义 TCP	20/21	地址段访问	0.0.0.0/0	1
	经典网络	公网							

说明:

- 部分运营商判断端口 135、139、444、445、5800、5900 等为高危端口并默认屏蔽。因此，即使 ECS 实例放行这些端口，在部分地区仍无法访问。建议您修改敏感端口为其它非高危端口承载业务。
- 更多关于 Windows 实例服务端口说明，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。

1.5 创建安全组

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。网络类型不同，安全组规则不同。如果您不希望您的实例加入默认安全组，您可以创建自定义安全组。

背景信息

每个ECS实例必须至少属于一个安全组。详细信息请参见*#unique_26*。

如果您在创建实例前未创建安全组，您可以使用默认安全组。默认安全组的规则，请参见安全组默认规则。

前提条件

如果您要创建专有网络类型安全组，您必须先创建专有网络和交换机。

> 说明:
> 专有网络类型的安全组，可以跨交换机，但不能跨专有网络。

操作步骤

1. 登录*ECS*管理控制台。
2. 在左侧导航栏中，选择 网络和安全 > 安全组。
3. 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：根据安全组中实例上需要部署的服务，选择合适的模板，简化安全组规则配置，如下表所示。

场景	模板	说明
安全组中的Linux实例上需要部署Web服务	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Windows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

没有特殊的需求	自定义	安全组创建成功后，根据需要的服务 添加安全组规则

- 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。
- 网络类型：
  - 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。
  - 如果为经典网络类型安全组，选择 经典网络。

6. 单击 确定。

对于您自己创建的安全组，在没有添加任何安全组规则之前，私网和公网默认规则均为：出方向允许所有访问，入方向拒绝所有访问。

API操作

您可以*#unique_29*接口创建安全组。

后续操作

- 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。安全组规则常用端口请参见*ECS*实例常用端口介绍，常用案例请参见安全组规则的典型应用。

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。

背景信息

如果以下场景的安全组规则不满足您的业务需求，您可以添加安全组规则。

- 创建实例时选择了默认安全组。
- 创建安全组时选择了Web Server Linux模板。
- 创建安全组时选择了Web Server Windows模板。
- 自定义模板。

使用须知

- 专有网络的安全组只需要设置出方向或入方向的规则，不区分内网和公网。专有网络安全组只能设置内网规则。您设置的安全组规则同时对内网和公网生效。
- 经典网络的安全组需要分别设置公网或内网的出方向或入方向规则。
- 所有的安全组，在未添加任何安全组规则之前，无论哪种网卡类型，出方向允许所有访问，入方向拒绝所有访问。

- 安全组规则的变更会自动应用到安全组内的ECS实例上。

前提条件

- 您已经创建了一个安全组，具体操作，请参见 创建安全组。
- 您已经知道自己的实例需要允许或禁止哪些公网或内网的访问。

操作步骤

1. 登录 云服务器ECS管理控制台。
2. 在左侧导航栏中，选择 网络和安全 > 安全组。
3. 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，单击 添加安全组规则。

   如果您不需要设置ICMP、GRE协议规则，或者您想使用下表中列出的协议的默认端口，单击快速创建规则。

协议	端口
SSH	22
telnet	23
HTTP	80
HTTPS	443
MS SQL	1433
Oracle	1521
MySQL	3306
RDP	3389
PostgreSQL	5432
Redis	6379

说明:

每个安全组的入方向规则与出方向规则的总数不能超过100条。

6. 在弹出的对话框中，设置以下参数：

- 网卡类型：
  - 如果是专有网络类型的安全组，不需要选择这个参数。需要注意以下信息：
    - 如果您的实例能访问公网，可以设置公网和内网的访问规则。
    - 如果您的实例不能访问公网，只能设置内网的访问规则。
  - 如果是经典网络的安全组，选择 公网 或 内网。
- 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。
- 授权策略：选择 允许 或 拒绝。

> 说明：
> 这里的 拒绝 策略是直接丢弃数据包，不给任何回应信息。如果2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，接受 授权不生效。

- 协议类型 和 端口范围：端口范围的设置受协议类型影响。下表是协议类型与端口范围的关系。

协议类型	端口范围	应用场景
全部	显示为-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）	显示为-1/-1，表示不限制端口。不能设置。	使用 `ping` 程序检测实例之间的通信状况。
全部GRE	显示为-1/-1，表示不限制端口。不能设置。	用于VPN服务。
自定义TCP 自定义UDP	自定义端口范围，有效的端口值是1 ~ 65535，端口范围的合法格式是开始端口/结束端口。即使是一个端口，也需要采用合法格式设置端口范围，比如：80/80表示端口80。	可用于允许或拒绝一个或几个连续的端口。
SSH	显示为22/22。 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。	用于SSH远程连接到Linux实例。
TELNET	显示为23/23。	用于Telnet远程登录实例。

协议类型	端口范围	应用场景
HTTP	显示为80/80。	实例作为网站或Web应用服务器。
HTTPS	显示为443/443。	实例作为支持HTTPS协议的网站或Web应用服务器。
MS SQL	显示为1433/1433。	实例作为MS SQL服务器。
Oracle	显示为1521/1521。	实例作为Oracle SQL服务器。
MySQL	显示为3306/3306。	实例作为MySQL服务器。
RDP	显示为3389/3389。 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。	实例是Windows实例，需要远程桌面连接实例。
PostgreSQL	显示为5432/5432。	实例作为PostgreSQL服务器。
Redis	显示为6379/6379。	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，但是您可以 申请解封端口25。其他常用端口信息，请参见 常用端口的典型应用。

- 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。

授权类型	授权对象
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实例访问本安全组中的实例，实现内网互通。 - 本账号授权：选择同一账号下的其他安全组ID。如果是专有网络的安全组，必须为同一个专有网络的安全组。 - 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。 因为安全组访问只对内网有效，所以，对专有网络实例，安全组访问的规则仅适用于内网访问，不适用于公网访问。公网访问只能通过 地址段访问 授权。

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。

- 优先级：1 ~ 100，数值越小，优先级越高。更多优先级信息，请参见 *ECS*安全组规则优先级说明。

7. 单击 确定，即成功地为指定安全组添加了一条安全组规则。

如果没有显示添加的安全组，单击 刷新 图标。

查看安全组规则是否生效

假设您在实例里安装了Web服务，并在一个安全组里添加了一条安全组规则：公网入方向，允许所有IP地址访问实例的TCP 80端口。

Linux实例

如果是安全组中的一台Linux实例，按以下步骤查看安全组规则是否生效。

1. *#unique_23*。
2. 运行以下命令查看TCP 80是否被监听。

```
netstat -an | grep 80
```

如果返回以下结果，说明TCP 80端口已开通。

```
tcp        0      0 0.0.0.0:80                  0.0.0.0:*
        LISTEN
```

3. 在浏览器地址栏里输入 `http://实例公网IP地址`。如果访问成功，说明规则已经生效。

Windows实例

如果是安全组中的一台Windows实例，按以下步骤查看安全组规则是否生效。

1. *#unique_24*。
2. 运行 命令提示符，输入以下命令查看TCP 80是否被监听。

```
netstat -aon | findstr :80
```

如果返回以下结果，说明TCP 80端口已开通。

```
TCP    0.0.0.0:80           0.0.0.0:0              LISTENING
1172
```

3. 在浏览器地址栏里输入 `http://实例公网IP地址`。如果访问成功，说明规则已经生效。

ECS安全组规则优先级说明

安全组规则的优先级可以设为1 ~ 100的任一个数值，数值越小，优先级越高。

ECS实例可以加入不同的安全组。无论是同一个安全组内或不同安全组之间，如果安全组规则互相矛盾，即协议类型、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 授权规则生效，接受 授权规则不生效。
- 如果 优先级 不同，则优先级高的规则生效，与 授权策略 的设置无关。

API操作

- 通过 *AuthorizeSecurityGroup* 接口增加一条安全组入方向规则。
- 通过 *AuthorizeSecurityGroupEgress* 接口增加一条安全组出方向规则。

后续操作

每个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。安全组规则的执行顺序与安全组规则的排序以及优先级有关，详情请参见 *ECS安全组中规则的优先级执行匹配顺序说明*。

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，一个 ECS 实例可以加入五个安全组。

背景信息

安全组用于设置单台或多台实例的网络访问控制，它是重要的网络安全隔离手段。每个实例至少属于一个安全组。

前提条件

- 您必须已经成功创建了 ECS 实例。
- 经典网络类型的实例必须加入同一地域下经典网络类型的安全组。
- 专有网络类型的实例必须加入同一专有网络下的安全组。

操作步骤

1. 登录云服务器 ECS 管理控制台。
2. 在左侧导航栏中，单击实例。
3. 选择地域。
4. 在实例列表页面中，找到需要加入安全组的实例，单击操作列下的管理。
5. 单击本实例安全组。
6. 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多个安全组，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，安全组的规则自动对实例进行生效。

相关API

您可以通过*JoinSecurityGroup*接口将一台实例加入到指定的安全组。

相关操作

- 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。
- 如果您不希望您的实例属于某个或某几个安全组，您可以将实例移出安全组。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。
- 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。

1.8 管理安全组

创建安全组后，您可以查询、修改、克隆、移出和删除安全组，以实现对安全组的精细化管理。

查询安全组列表

1. 登录云服务器 ECS 管理控制台。
2. 单击左侧导航栏中的安全组。
3. 选择地域，会展示该地域下的所有安全组。

4. （可选）查询您所需要的安全组。
   - 在筛选输入框输入安全组 ID可查询到该 ID 对应的安全组。
   - 在筛选输入框输入专有网络 ID可查询到该专有网络下的所有安全组。
   - 在筛选输入框输入安全组名称可查询到该名称对应的安全组。

您也可以通过*DescribeSecurityGroups*接口查询安全组的基本信息（安全组 ID 和安全组描述等）。

修改安全组属性

1. 登录云服务器 *ECS* 管理控制台。
2. 单击左侧导航栏中的安全组。
3. 选择地域。
4. 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。

您也可以通过*ModifySecurityGroupAttribute*接口修改指定安全组的属性，包括修改安全组名称和描述。

克隆安全组

1. 登录云服务器 *ECS* 管理控制台。
2. 在左边导航栏里，单击安全组。
3. 选择地域。
4. 在安全组列表里，找到需要克隆的安全组，在操作列中，单击克隆。
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. 确认无误后，单击确定。

移出安全组

1. 登录云服务器 *ECS* 管理控制台。
2. 在左侧导航栏中，单击实例。
3. 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。

您也可以使用*LeaveSecurityGroup*接口将一台实例移出指定的安全组。

删除安全组

1. 登录云服务器 *ECS* 管理控制台。
2. 在左侧导航栏里，选择网络和安全 > 安全组。
3. 选择地域。
4. 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。

您也可以通过*#unique_47*接口删除安全组。

1.9 管理安全组规则

添加安全组规则后，您可以查询、修改、还原、导出、导入或删除安全组规则，以实现对安全组规则的精细化管理。

查询安全组规则

前提条件

您的安全组中已添加安全组规则。

操作步骤

1. 登录云服务器 *ECS* 管理控制台。
2. 单击左侧导航中的安全组。
3. 选择地域。
4. 找到想要查询的安全组，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，您可以选择入方向或出方向。
   - 如果您需要查询改经典网络类型的安全组规则您可以请选择内网入方向、内网出方向、公网入方向或公网出方向。

您也可以通过*DescribeSecurityGroupAttribute*接口查询安全组详情。

修改安全组规则

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。

前提条件

您必须已经创建了安全组，并在安全组中添加了安全组规则。

操作步骤

1. 登录云服务器 ECS 管理控制台。
2. 单击左侧导航栏中的安全组。
3. 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。

还原安全组规则

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。

使用限制

- 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。
- 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）。

前提条件

在同一地域下，同一种网络类型下，您应该拥有至少一个安全组。

操作步骤

1. 登录云服务器 ECS 管理控制台。
2. 单击左侧导航栏里的安全组。
3. 选择地域。
4. 在安全组列表里，找到需要还原规则的安全组作为原安全组，单击操作列下的还原规则。
5. 在还原规则对话框里：

   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，您应该选择全部还原。
      - 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，您应该选择部分还原。

   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。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。

导出安全组规则

1. 登录云服务器 ECS 管理控制台。
2. 单击左侧导航栏中的安全组。
3. 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。

    说明：

   JSON 文件命名规则示例：

   ecs_${region_id}_${groupID}.json

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

导入安全组规则

1. 登录云服务器 ECS 管理控制台。
2. 登录云服务器 ECS 管理控制台。
3. 单击左侧导航栏中的安全组。
4. 选择地域。

   说明:
   安全组支持导入不同地域的安全组规则。
5. 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。
6. 单击导入规则。
7. 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100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。
8. 单击开始导入。
9. 查看导入安全组规则的结果，单击导入结束，关闭。

删除安全组规则

1. 登录云服务器 ECS 管理控制台。
2. 单击左侧导航栏里的安全组。
3. 选择安全组所在的地域。
4. 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。

您也可以通过RevokeSecurityGroup接口删除一条安全组入方向规则或通过RevokeSecurityGroupEgress接口删除一条安全组出方向规则。

1.10 安全组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。

每个实例至少属于一个安全组，在创建的时候就需要指定。同一安全组内的实例之间网络互通，不同安全组的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。

如果您在购买 ECS 实例时不选择安全组，创建的 ECS 实例都会分配到一个固定的安全组，您还需要重新通过移出安全组以及加入新的安全组来实现网络安全隔离。

为什么专有网络实例不能设置公网安全组规则?

专有网络（VPC）实例的公网访问通过内网网卡映射完成，您在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。更多应用，请参见安全组应用案例。

为什么还是无法访问 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。

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。

为什么实例加入安全组时提示：规则数量超限?

作用于一个实例（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，说明实际作用于当前实例上的规则总数已经超过数量上限。

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。

安全组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。

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。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。

说明:

目前，一个实例中的每个弹性网卡默认最多可以加入 5 个安全组，所以一个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。

VPC 类型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 VPC 类型实例的安全组都生效。

2 SSH密钥对

2.1 SSH 密钥对

SSH 密钥对，常简称为密钥对，是区别于用户名加密码的远程登录 Linux 实例认证方式。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。一个对外界公开，称为 公钥，另一个您自己保留，称为 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：

- 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。

说明：

- 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。

- ECS 会保存密钥对的公钥部分。
- 密钥对创建成功后，您需要妥善保管私钥。
- 基于数据安全考虑，在实例状态为 运行中 （Running） 绑定或者解绑密钥对时，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。

   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

相关操作

- 创建 SSH 密钥对。
- 导入 SSH 密钥对。
- 删除 SSH 密钥对。
- 绑定和解绑 SSH 密钥对。
- 创建实例 时指定 SSH 密钥对。
- #unique_78。

2.2 使用SSH密钥对

本文提供了在ECS控制台上使用SSH密钥对的操作指示。SSH密钥对仅支持Linux实例。

创建SSH密钥对

1. 登录ECS管理控制台。
2. 在左侧导航栏中，单击密钥对。
3. 选择地域。
4. 单击创建密钥对。
5. 设置密钥对名称，并选择自动新建密钥对。

> 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. 单击确定创建密钥对。

> 说明:
> - 创建密钥对后，请务必下载并妥善保管私钥。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。
> - 一个账号在一个地域最多可以拥有500个密钥对。

相关API：*CreateKeyPair*

查看公钥信息

本地为Windows操作系统

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 AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6vYrExwT4WU4
fsaRcVXGV2Mg9RHex21hl1au77GkmnIgukBZjywlQOT4GDdsJy2nBOdJPrCEBIP6t0Mk5a
PkK/fctNuKjcmMMOA8YUT+sJKn3l7rCLkesE+S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGM
```

```
XZQPpkBtojcV14uAy0yV6/htEqGa/Jq4fH7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKu
IHdMWOPvjGACGcXclex+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。

导入SSH密钥对

除了新建密钥对之外，您也可以使用工具生成SSH密钥对并将公钥导入阿里云。

说明:

不要导入私钥。请您妥善保存私钥。

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

1. 获取公钥信息。详细步骤，请参见查看公钥信息。
2. 登录ECS管理控制台。
3. 在左侧导航栏中，单击密钥对。
4. 选择地域。
5. 单击创建密钥对。

6. 设置密钥对名称，选择导入已有密钥对，并在公钥内容中输入公钥信息。

> 说明:
> 指定的名称不应该与已有的密钥对名称重复，也不应该与删除前仍绑定实例的密钥对名称重复，否则，控制台会提示密钥对已存在。

7. 单击确定。

相关API：*ImportKeyPair*

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。

> 说明:
> - 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。
> - 如果ECS实例使用密码认证，绑定密钥对后，密码验证方式自动失效。但如果在绑定密钥对之后重置实例密码，除使用密钥对方式之外，您也可以使用密码方式登录实例。

1. 登录ECS管理控制台。
2. 在左侧导航栏中，单击密钥对。
3. 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>，移入已选择栏中。

> 说明:
> 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。

> 说明:
> 如果ECS实例处于运行中（Running）状态，绑定SSH密钥对后，您必须在控制台或者使用API重启实例，才能使操作生效。

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。

相关API：*AttachKeyPair*

解绑SSH密钥对

1. 登录ECS管理控制台。
2. 在左侧导航栏中，单击密钥对。
3. 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>，移入已选择栏中。
6. 单击确定。

> 说明：
>
> - 如果ECS实例处于运行中（Running）状态，解绑SSH密钥对后，您必须在控制台或者使用API重启实例，才能使操作生效。
> - 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使用密码方式登录。如果解绑密钥对之前没有重置实例密码，则解绑密钥对之后，必须重置实例密码才能使用密码方式登录实例。

相关API：*DetachKeyPair*

在实例内添加或替换密钥对

您可以在实例内添加多个密钥对，允许多个密钥对访问该实例。您也可以替换现有的密钥对。

1. 获取新密钥对的公钥信息。详细步骤，请参见查看公钥信息。
2. 使用现有的密钥对连接ECS实例。
3. 运行`vim .ssh/authorized_keys`命令打开文件。
4. 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/bUUduZjauiJa1KQJSF4+czKtqMAv38QEspiWStkSfpTn1g9qeUhfKd4uWlmx
eQ+XjPsf22fRem+v7MHMa7KnZWiHJxO62D4Ihvv2hKfskz8K44mVMeInMjGO+
u17IaL2l2ri8q9YdvVHt0Mw5TpCkERWGoBPE1Y8vxFb97TaE5+zc+2+eff6PDCMkV
TP+c/feMeCxpx6Lhc2NEpHIPxMpjOv1IytKiDfWcezA2aCmKre0Q2t/YudCmJ8HTC
nLId5LpirbNE4X08Bk7tXZAU8UaoeDdUr/FKB1Cxw1TbGMTfWBcdWkdp2lv
imported-openssh-key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdlrdZwV3+GF9q7rhc6v
YrExwT4WU4fsaRcVXGV2Mg9RHex21hl1au77GkmnIgukBZjywlQOT4GDdsJy
2nBOdJPrCEBIP6t0Mk5aPkK/fctNuKjcmMMOA8YUT+sJKn3l7rCLkesE+
S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcV14uAy0yV6/htEqGa
/Jq4fH7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKuIHdMWOPvjGACGcXclex+
```

```
lHtTGiAIRG1riyNRVC47ZEVCg9iTWWGrWFvVlnI0E3Deb/9H9mPCO1Xt2fxxxxxxxx
BtmR imported-openssh-key
```

- 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+GF9q7rhc6v
YrExwT4WU4fsaRcVXGV2Mg9RHex21hl1au77GkmnIgukBZjywlQOT4GDdsJy
2nBOdJPrCEBIP6t0Mk5aPkK/fctNuKjcmMMOA8YUT+sJKn3l7rCLkesE+
S5880yNdRjBiiUy40kyr7Y+fqGVdSOHGMXZQPpkBtojcV14uAy0yV6/htEqGa
/Jq4fH7bR6CYQ2XgH/hCap29Mdi/G5Tx1nbUKuIHdMWOPvjGACGcXclex+
lHtTGiAIRG1riyNRVC47ZEVCg9iTWWGrWFvVlnI0E3Deb/9H9mPCO1Xt2fxxxxxxxx
BtmR imported-openssh-key
```

如果能够使用新的私钥登录ECS实例，表示添加或者替换密钥对成功。

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。

> **说明:**
>
> - 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。

1. 登录ECS管理控制台。
2. 在左侧导航栏中，单击密钥对。
3. 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API：*DeleteKeyPairs*

3 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 云盾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。

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
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

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.r5.6xlarge	7500	1500000
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

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.i2.2xlarge	2000	1000000
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

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.gn5-c28g1.14xlarge	10000	4500000
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

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.t5-c1m1.2xlarge	1200	400000
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

实例规格	最大BPS清洗阈值（Mbit/s）	最大PPS清洗阈值（PPS）
ecs.n4.8xlarge	5000	500000
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。

4 实例RAM角色

4.1 什么是实例 RAM 角色

ECS 实例 RAM（Resource Access Management） 角色（以下简称实例 RAM 角色）是 RAM 角色的一种，它让 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。

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。

背景信息

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 （AccessKeyId + AccessKeySecret）访问阿里云各产品的 API。

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，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） 网络类型的实例才能使用实例角色。
- 一个 ECS 实例一次只能授予一个实例 RAM 角色。

使用实例 RAM 角色

目前有两种使用 RAM 角色的方式：

- 通过控制台使用实例RAM角色
- 通过API使用实例RAM角色

参考链接

- 您可以参阅 支持 RAM 的云服务 了解支持 STS 临时凭证的云服务。
- 您可以参阅 借助于实例 RAM 角色访问其他云产品 了解如何访问其他云产品的 API 。

4.2 通过控制台使用实例 RAM 角色

您可在控制台创建、授权实例RAM角色，并将其授予实例。

使用限制

使用实例 RAM 角色存在如下限制：

- 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 #unique_98 获取实例 RAM 角色的临时授权 Token。参阅 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。

前提条件

您已经开通 RAM 服务，参阅 RAM 文档 开通方法 开通 RAM 服务。

1. 创建实例 RAM 角色

1. 登录 RAM 控制台。
2. 在导航窗格中，单击 角色管理。
3. 在角色管理页面，单击 新建角色。

4. 在弹窗中：

   a. 角色类型 选择 服务角色。

   b. 类型信息 选择 ECS 云服务器。

   c. 输入角色名称及备注，如 EcsRamRoleDocumentTesting。

   d. 单击 创建。

2. 授权实例 RAM 角色

1. 登录 *RAM* 控制台。
2. 在导航窗格中，单击 策略管理。
3. 在 策略管理 页面，单击 新建授权策略。
4. 在弹窗中：

   a. 权限策略模板 选择 空白模板。

   b. 输入 授权策略名称 及 策略内容，如 EcsRamRoleDocumentTestingPolicy。

   > 说明：
   > 关于如何编写策略内容，您可以参阅 RAM 文档 *Policy*语法结构。

   c. 单击 新建授权策略 完成授权。
5. 在导航窗格中，单击 角色管理。
6. 在 角色管理 页面，选择创建好的角色，如 EcsRamRoleDocumentTesting，单击 授权。
7. 输入创建的 授权策略名称，如 EcsRamRoleDocumentTestingPolicy。
8. 单击符号 > 选中策略名，单击 确定。

3. 授予实例 RAM 角色

1. 登录 *ECS*管理控制台。
2. 在导航窗格中，单击 实例。
3. 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，如 EcsRamRoleDocumentTesting，单击 确定 完成授予。

4. （可选）收回实例 RAM 角色

   1. 登录 ECS管理控制台。
   2. 在导航窗格中，单击 实例。
   3. 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。

5. （可选）更换实例 RAM 角色

   1. 登录 ECS管理控制台。
   2. 在导航窗格中，单击 实例。
   3. 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。

6. （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。示例：

   1. 远程连接并登录到 ECS 实例。
   2. 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：参阅 #unique_98。
   3. 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"
```

```
}
```

7. （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。

登录 RAM 控制台，参阅 为 RAM 用户授权 完成授权，授权策略如下所示：

```
{
        "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，请参阅 鉴权规则。

参考链接

- 您也可以 通过API使用实例RAM角色。
- 您也许想 借助实例 RAM 角色访问其它云产品 API。

4.3 通过 API 使用实例 RAM 角色

使用限制

使用实例 RAM 角色存在如下限制：

- 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 #unique_98 获取实例 RAM 角色的临时授权 Token。参阅 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。

前提条件

您已经开通 RAM 服务，参阅 RAM 文档 开通方法 开通 RAM 服务。

1. 创建实例 RAM 角色

1. 调用接口 CreateRole 创建实例 RAM 角色。
2. 设置 RoleName 参数，如将其值置为 EcsRamRoleDocumentTesting。
3. 按如下策略设置 AssumeRolePolicyDocument：

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

2. 授权实例 RAM 角色

1. 调用接口 CreatePolicy 新建授权策略。
2. 设置 RoleName 参数，如将其值置为 EcsRamRoleDocumentTestingPolicy。
3. 按如下策略设置 PolicyDocument：

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

4. 调用接口 AttachPolicyToRole 授权角色策略。
5. 设置 PolicyType 参数为 Custom。
6. 设置 PolicyName 参数，如 EcsRamRoleDocumentTestingPolicy。

7. 设置 RoleName 参数，如 EcsRamRoleDocumentTesting。

3. 授予实例 RAM 角色

1. 调用接口 *#unique_111* 为实例授予 RAM 角色。
2. 设置 RegionId 及 InstanceIds 参数指定一个 ECS 实例。
3. 设置 RamRoleName 参数，如 EcsRamRoleDocumentTesting。

4. （可选）收回实例 RAM 角色

1. 调用接口 *#unique_112* 收回实例 RAM 角色。
2. 设置 RegionId 及 InstanceIds 参数指定一个 ECS 实例。
3. 设置 RamRoleName 参数，如 EcsRamRoleDocumentTesting。

5. （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。示例：

1. 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：参阅文档 *#unique_98*。
2. 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"
}
```

6. （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。

登录 RAM 控制台，参阅文档 为 *RAM* 用户授权 完成授权，如下所示：

```
{
        "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，请参阅 鉴权规则。

参考链接

- 您也可以 通过控制台使用实例RAM角色。
- 您也许想 借助于实例 RAM 角色访问其他云产品。
- 实例 RAM 角色相关的 API 接口包括：
  - 创建 RAM 角色：*CreateRole*
  - 查询 RAM 角色列表：*ListRoles*
  - 新建 RAM 角色策略：*CreatePolicy*
  - 授权 RAM 角色策略：*AttachPolicyToRole*
  - 授予实例 RAM 角色：*#unique_111*
  - 收回实例 RAM 角色：*#unique_112*
  - 查询实例 RAM 角色：*#unique_114*