ALIBABA CLOUD

阿里云

专有网络VPC

网络ACL

文档版本：20210118

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。

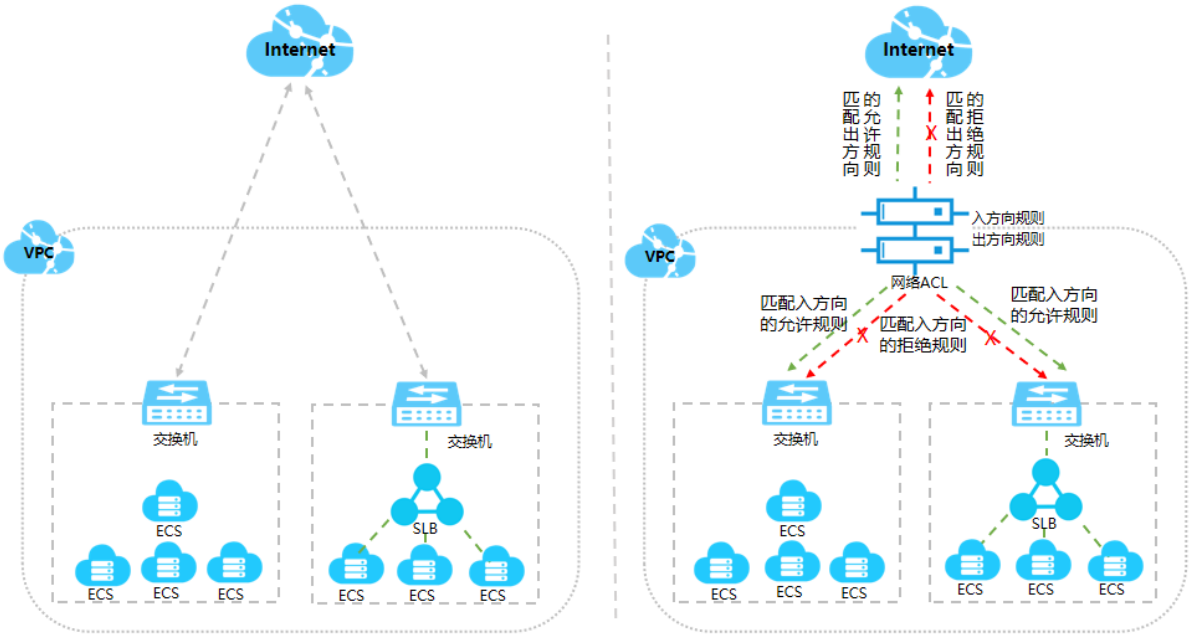
通用约定

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.网络ACL概述

网络ACL（Network Access Control List）是专有网络VPC中的网络访问控制功能。您可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中云服务器ECS实例的流量的访问控制。



功能发布及地域支持情况

网络ACL功能默认支持的地域如下表所示。

区域	支持网络ACL的地域
亚太	华北5（呼和浩特）、华北6（乌兰察布）、华南2（河源）、华南3（广州）、西南1（成都）、印度尼西亚（雅加达）
欧洲与美洲	英国（伦敦）
中东与印度	印度（孟买）

网络ACL功能正在公测的地域如下表所示，请可以提交公测申请。

区域	支持网络ACL的地域
亚太	华北1（青岛）、华北2（北京）、华北3（张家口）、华东1（杭州）、华东2（上海）、华南1（深圳）、中国（香港）、日本（东京）、新加坡、澳大利亚（悉尼）、马来西亚（吉隆坡）
欧洲与美洲	美国（硅谷）、德国（法兰克福）
中东与印度	阿联酋（迪拜）

功能特性

网络ACL具有以下特性：

- 网络ACL规则仅过滤绑定的交换机中的ECS实例的流量（包括负载均衡SLB转发给ECS实例的流量）。

  > **说明** 如果您的ECS实例绑定了辅助弹性网卡，且辅助弹性网卡绑定了设置网卡可见模式的EIP，那么网络ACL不过滤该ECS实例的流量。更多信息，请参见设置EIP网卡可见模式。

- 网络ACL的规则是无状态的，即设置入方向规则的允许请求后，需要同时设置相应的出方向规则，否则可能会导致请求无法响应。
- 网络ACL无任何规则时，会拒绝所有出入方向的访问。
- 网络ACL与交换机绑定，不过滤同一交换机内的ECS实例间的流量。

规则说明

您可以在网络ACL中添加或删除规则，更改规则后会自动应用到与其绑定的交换机。新创建的网络ACL，默认会在出方向和入方向分别生成一条规则，表示允许所有出、入方向流量。您可以删除默认规则。出方向和入方向默认规则如下所示。

- 入方向规则

生效顺序	协议类型	源地址	目的端口范围	策略	类型
1	all	0.0.0.0/0	-1/-1	允许	自定义

- 出方向规则

生效顺序	协议类型	目标地址	目的端口范围	策略	类型
1	all	0.0.0.0/0	-1/-1	允许	自定义

网络ACL中的元素说明如下：

- 生效顺序：值越小，规则的优先级越高。 系统从生效顺序为1的规则开始判断，只要有一条规则与流量匹配，即应用该规则，并忽略其他规则。

  例如，ECS实例请求访问目的地址为172.16.0.1的数据包，在经过如下表所示的ACL规则配置后，172.16.0.1匹配生效顺序2和生效顺序3规则中的目的地址，由于生效顺序2的优先级高于生效顺序3，所以会根据生效顺序2规则拒绝该请求。

生效顺序	协议类型	目标地址	目的端口范围	策略	类型
1	all	10.0.0.0/8	-1/-1	允许	自定义
2	all	172.16.0.0/12	-1/-1	拒绝	自定义
3	all	172.16.0.0/12	-1/-1	允许	自定义

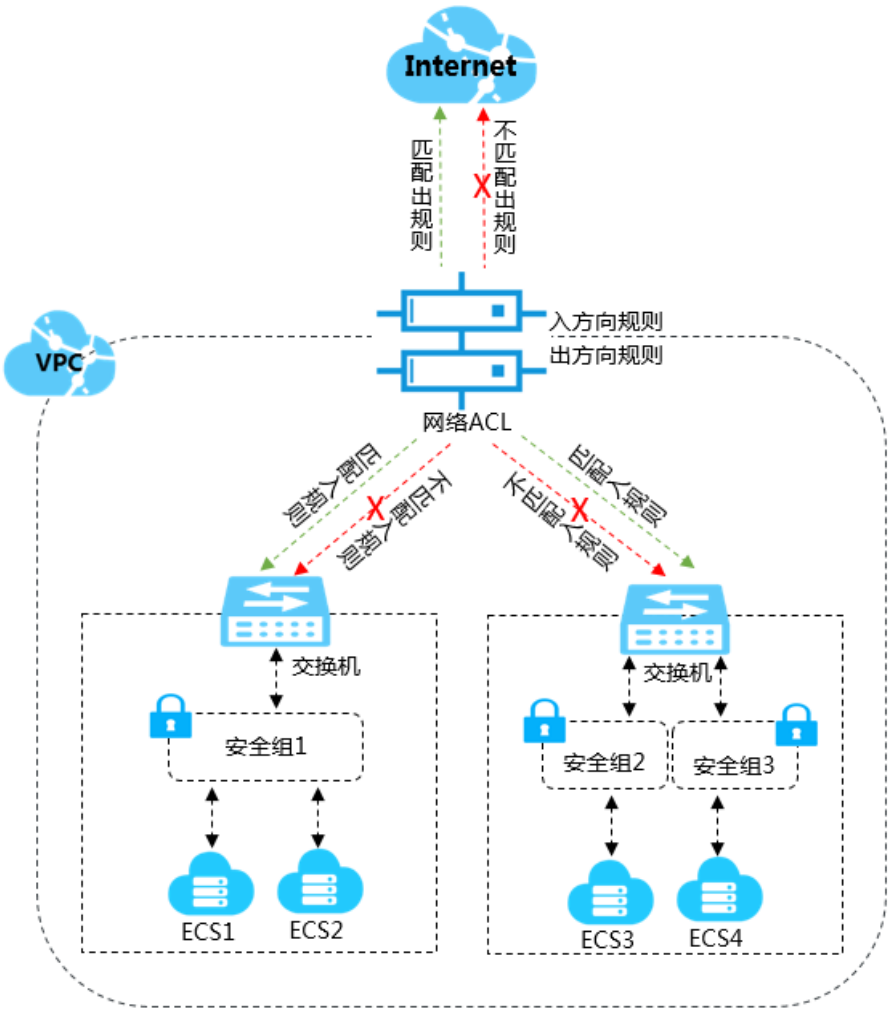
- 策略：针对特定流量选择允许或拒绝。
- 协议类型：指定协议的类型，可选择all、icmp、gre、tcp和udp。
- 源地址（限入方向规则）：数据流的源地址。
- 目标地址（限出方向规则）：数据流的目标地址。
- 目的端口范围（限入方向规则）：入方向规则作用的端口范围。
- 目的端口范围（限出方向规则）：出方向规则作用的端口范围。

网络ACL与安全组

与交换机绑定的网络ACL规则控制允许进入交换机的数据流，与ECS实例相关的安全组规则控制允许进入ECS实例的数据流。网络ACL和安全组的基本差异如下表所示。

网络ACL	安全组
在交换机级别运行。	在实例级别运行。
无状态：返回数据流必须被规则明确允许。	有状态：返回数据流会被自动允许，不受任何规则的影响。
不评估所有规则，按照规则的生效顺序处理所有规则。	执行规则前，会评估所有规则。
ECS实例所属的交换机仅允许绑定一个网络ACL。	一个ECS实例可加入多个安全组。

网络ACL和安全组提供的安全层如下所示。



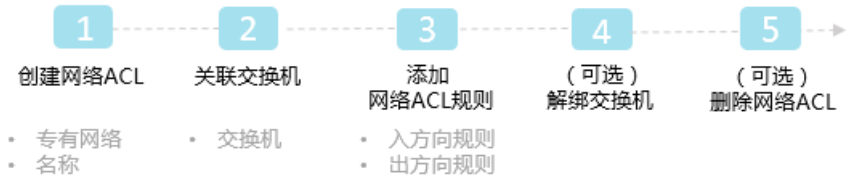
使用限制

网络ACL具有以下限制。

资源	默认限制	提升配额
单个VPC支持创建的网络ACL数量	200个	无法提升。
单个交换机支持绑定的网络ACL数量	1个	
单个网络ACL支持创建的规则数量	• 入方向规则20条 • 出方向规则20条	您可以通过以下任意方式自助提升配额： • 前往配额管理页面提升配额，具体操作，请参见管理配额。 • 前往配额中心提升配额。具体操作，请参见创建配额提升申请。
不支持创建网络ACL的VPC	VPC中含有以下实例规格族中的任一实例： ecs.c1、ecs.c2、ecs.c4、ecs.ce4、ecs.cm4、ecs.d1、ecs.e3、ecs.e4、ecs.ga1、ecs.gn4、ecs.gn5、ecs.i1、ecs.m1、ecs.m2、ecs.mn4、ecs.n1、ecs.n2、ecs.n4、ecs.s1、ecs.s2、ecs.s3、ecs.se1、ecs.sn1、ecs.sn2、ecs.t1、ecs.xn4 更多信息，请参见VPC高级功能概述。	升级不支持VPC高级功能的ECS实例的规格或释放不支持VPC高级功能的ECS实例。 • 升级操作，请参见包年包月实例升配规格和按量付费实例变配规格。 • 释放操作，请参见释放实例。 说明 如果您的VPC中含有ECS实例规格族限制中的任一实例，且您已经创建了网络ACL，为了保证正常使用网络ACL功能，请升级ECS实例规格或释放ECS实例。

使用流程

网络ACL的使用流程图如下所示。



具体操作，请参见：

- 限制不同交换机下的ECS间的互通。
- 限制本地数据中心与云上的互通。

2.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网络ACL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

常用端口及服务如下表所示。

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。
25	SMTP	SMTP服务所开放的端口，用于发送邮件。
80	HTTP	用于HTTP服务提供访问功能，例如，IIS、Apache、Nginx等服务。
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是用于接收电子邮件的协议。
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，8080端口常用于WWW代理服务，实现网页浏览。

自定义网络ACL

入方向规则和出方向规则显示了一个仅支持IPv4的VPC的网络ACL示例。其中：

- 生效顺序1、2、3、4的入方向规则分别为允许HTTP、HTTPS、SSH、RDP数据流进入交换机的规则，出方向响应规则为生效顺序3的出方向规则。
- 生效顺序1、2的出方向规则分别为允许HTTP和HTTPS流量离开交换机的规则，入方向响应规则为生效顺序5的入方向规则。
- 生效顺序6的入方向规则为拒绝所有入方向IPv4流量，该规则会确保在数据包不匹配任何其他规则时拒绝

此数据包。

- 生效顺序4的出方向规则为拒绝所有出方向IPv4流量，该规则会确保在数据包不匹配任何其他规则时拒绝此数据包。

> **说明** 无论是入方向规则还是出方向规则，请确保每一条规则都存在允许响应流量的相应入方向或出方向规则。

入方向规则

生效顺序	协议类型	源地址	目的端口范围	策略	说明
1	tcp	0.0.0.0/0	80/80	允许	允许来自任意IPv4地址的入方向HTTP流量。
2	tcp	0.0.0.0/0	443/443	允许	允许来自任意IPv4地址的入方向HTTPS流量。
3	tcp	0.0.0.0/0	22/22	允许	允许来自任意IPv4地址的入方向SSH流量。
4	tcp	0.0.0.0/0	3389/3389	允许	允许来自任意IPv4地址的入方向RDP流量。
5	tcp	0.0.0.0/0	32768/65535	允许	允许来自互联网的入方向返回IPv4流量。 此端口范围仅为示例。有关如何选择适当的临时端口的更多信息，请参见临时端口。
6	all	0.0.0.0/0	-1/-1	拒绝	拒绝所有入方向IPv4流量。

出方向规则

生效顺序	协议类型	目标地址	目的端口范围	策略	说明
1	tcp	0.0.0.0/0	80/80	允许	允许出方向IPv4 HTTP流量从交换机流向互联网。
2	tcp	0.0.0.0/0	443/443	允许	允许出方向IPv4 HTTPS流量从交换机流向互联网。
3	tcp	0.0.0.0/0	32768/65535	允许	允许对互联网客户端的出站IPv4响应。 此端口范围仅为示例。有关如何选择适当的临时端口的更多信息，请参见临时端口。
4	all	0.0.0.0/0	-1/-1	拒绝	拒绝所有出方向IPv4流量。

负载均衡的网络ACL

绑定网络ACL的交换机中的ECS作为负载均衡SLB的后端服务器时，您需要添加如下网络ACL规则。

- 入方向规则

生效顺序	协议类型	源地址	目的端口范围	策略	说明
1	SLB监听协议	允许接入SLB的客户端IP	SLB监听端口	允许	在SLB监听端口上允许来自指定客户端IP的入方向流量。
2	健康检查协议	100.64.0.0/10	健康检查端口	允许	在健康检查端口上允许来自健康检查地址的入方向流量。

- 出方向规则

生效顺序	协议类型	目标地址	目的端口范围	策略	说明
1	all	允许接入SLB的客户端IP	-1/-1	允许	允许所有流向指定客户端IP的出方向流量。
2	all	100.64.0.0/10	-1/-1	允许	允许所有流向健康检查地址的出方向流量。

临时端口

不同类型的客户端发起请求时使用的端口不同，您需要根据自己使用的或作为通信目标的客户端的类型为网络ACL使用不同的端口范围。常用客户端的临时端口范围如下。

客户端	端口范围
Linux	32768/61000
Windows Server 2003	1025/5000
Windows Server 2008及更高版本	49152/65535
NAT网关	1024/65535

3.创建网络ACL

网络ACL是专有网络VPC中的网络访问控制功能。您可以在专有网络VPC中创建网络ACL。

前提条件

您已经创建了专有网络。具体操作，请参见创建专有网络。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择要创建网络ACL的地域。网络ACL功能支持的地域信息，请参见功能发布及地域支持情况。
4. 在**网络ACL**页面，单击**创建网络ACL**。
5. 在**创建网络ACL**面板，根据以下信息配置网络ACL，然后单击**确定**。

配置	说明
专有网络	选择网络ACL所属的专有网络。 **说明** 要关联的专有网络的地域必须与网络ACL的地域相同。 如果专有网络中含有以下ECS实例规格族中的任一实例，则不支持为该专有网络创建网络ACL。 ecs.c1、ecs.c2、ecs.c4、ecs.ce4、ecs.cm4、ecs.d1、ecs.e3、ecs.e4、ecs.ga1、ecs.gn4、ecs.gn5、ecs.i1、ecs.m1、ecs.m2、ecs.mn4、ecs.n1、ecs.n2、ecs.n4、ecs.s1、ecs.s2、ecs.s3、ecs.se1、ecs.sn1、ecs.sn2、ecs.t1、ecs.xn4 如需创建网络ACL，请升级不支持VPC高级功能的ECS实例的规格或释放不支持VPC高级功能的ECS实例。 更多关于VPC高级功能的信息，请参见VPC高级功能概述。 ○ 如何升级，请参见包年包月实例升配规格或按量付费实例变配规格。 ○ 如何释放，请参见释放实例。 **说明** 如果您的VPC中含有ECS实例规格族限制中的任一实例，且您已经创建了网络ACL，为了保证正常使用网络ACL功能，请升级ECS实例规格或释放ECS实例。
名称	网络ACL的名称。 名称长度为2~128个字符，以英文字母或中文开头，可包含数字、下划线（_）和短划线（-）。
描述	网络ACL的描述。 描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

后续步骤

- 绑定交换机

- 添加入方向规则
- 添加出方向规则

相关文档

- CreateNetworkAcl

4.绑定交换机

创建网络ACL后，您可以将网络ACL与交换机绑定，实现对交换机中ECS实例流量的访问控制。

前提条件

将网络ACL绑定到交换机前，请确保满足以下条件：

- 您已经创建了网络ACL。具体操作，请参见创建网络ACL。
- 您已经创建了交换机，且交换机所属的VPC与要绑定的网络ACL所属的VPC相同。具体操作，请参见创建交换机。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**管理**。
5. 在**已绑定资源**页签下，单击**关联资源**。
6. 在**关联资源**面板，选择需要绑定的交换机，然后单击**确定**。

> **说明** 网络ACL仅允许绑定所属VPC内的交换机，且每个交换机仅允许绑定一个网络ACL。

后续步骤

- 添加入方向规则
- 添加出方向规则

相关文档

- AssociateNetworkAcl

5.添加网络ACL规则

5.1. 添加入方向规则

创建网络ACL后，您可以为网络ACL添加入方向规则，管控公网或私网对交换机中ECS实例的访问。

前提条件

您已经创建了网络ACL。具体操作，请参见创建网络ACL。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**设置入方向规则**。
5. 在**设置入方向规则**页签下，单击**创建入方向规则**。
6. 在**创建入方向规则**面板，根据以下信息配置入方向规则，然后单击**确定**。

配置	说明
名称	入方向规则的名称。 长度为2~128个字符，必须以字母或中文开头，可包含数字、下划线（_）和短划线（-），但不能以 `http://` 或 `https://` 开头。
生效顺序	入方向规则的生效顺序。 可输入数字1~20，数字越小，优先级越高。更多信息，请参见规则生效顺序。
策略	选择入方向规则的授权策略： ○ **允许**：允许访问交换机中ECS实例。 ○ **拒绝**：拒绝访问交换机中ECS实例。
协议类型	选择传输层协议，支持选择以下协议： ○ **ALL**：所有协议。 ○ **ICMP**：网络控制报文协议。 ○ **GRE**：通用路由封装协议。 ○ **TCP**：传输控制协议。 ○ **UDP**：用户数据报协议。
源地址	数据流的源地址网段。 默认为0.0.0.0/32。

配置	说明
目的端口范围	输入目的端口范围。 端口范围为1~65535，使用斜线（/）隔开起始端口和终止端口，格式为1/200、80/80，其中-1/-1不能单独设置，代表不限制端口。

相关文档

- UpdateNetworkAclEntries

5.2. 添加出方向规则

创建网络ACL后，您可以为网络ACL添加出方向规则，管控交换机中的ECS实例对公网或私网的访问。

前提条件

您已经创建了网络ACL。具体操作，请参见创建网络ACL。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**设置出方向规则**。
5. 在**出方向规则**页签下，单击**创建出方向规则**。
6. 在**创建出方向规则**面板，根据以下信息配置出方向规则，然后单击**确定**。

配置	说明
名称	出方向规则的名称。 名称长度为2~128个字符，必须以字母或中文开头，可包含数字、下划线（_）和短划线（-），但不能以 `http://` 或 `https://` 开头。
生效顺序	出方向规则的生效顺序。 可输入数字1~20，数字越小，优先级越高。更多信息，请参见规则生效顺序。
策略	选择出方向规则的授权策略： ○ **允许**：允许交换机中的ECS实例访问公网或私网。 ○ **拒绝**：拒绝交换机中的ECS实例访问公网或私网。

配置	说明
协议类型	选择传输层协议，支持选择以下协议： ○ **ALL**：所有协议。 ○ **ICMP**：网络控制报文协议。 ○ **GRE**：通用路由封装协议。 ○ **TCP**：传输控制协议。 ○ **UDP**：用户数据报协议。
目标地址	数据流的目标地址网段。 默认为0.0.0.0/32。
目的端口范围	输入目的端口范围。 端口范围为1~65535，使用斜线（/）隔开起始端口和终止端口，格式为1/200、80/80，其中-1/-1不能单独设置，代表不限制端口。

相关文档

- UpdateNetworkAclEntries

5.3. 调整规则顺序

网络ACL按照规则生效顺序执行规则，生效顺序的值越小，优先级越高。您可以为规则排序来指定规则执行的先后顺序。

调整入方向规则顺序

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**管理**。
5. 单击**入方向规则**页签，然后单击**排序**。
6. 在**排序**面板，上下拖动规则，然后单击**确定**。

> **说明** 规则顺序越上，优先级越高。

调整出方向规则顺序

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**管理**。
5. 单击**出方向规则**页签，然后单击**排序**。
6. 在**排序**面板，上下拖动规则，然后单击**确定**。

> **说明** 规则顺序越上，优先级越高。

相关文档

- 添加入方向规则
- 添加出方向规则

6.解绑交换机

您可以解除网络ACL与交换机的绑定关系，解除后，网络ACL将不再管控交换机中的ECS实例的流量。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**管理**。
5. 在**已绑定资源**页签下，找到需要解绑网络ACL的交换机，单击**操作**列下的**解绑**。
6. 在**解绑网络ACL**对话框中，单击**确定**。

相关文档

- UnassociateNetworkAcl

7.删除网络ACL

您可以删除一个不需要的网络ACL。

前提条件

确保要删除的网络ACL未绑定任何交换机，如有绑定，请先解除与交换机的绑定。具体操作，请参见解绑交换机。

操作步骤

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**删除**。
5. 在**删除网络ACL**对话框中，单击**确定**。

相关文档

- DeleteNetworkAcl

8.最佳实践

8.1. 限制不同交换机下的ECS间的互通

本文为您介绍如何通过网络ACL功能限制不同交换机下的ECS实例的互通。

前提条件

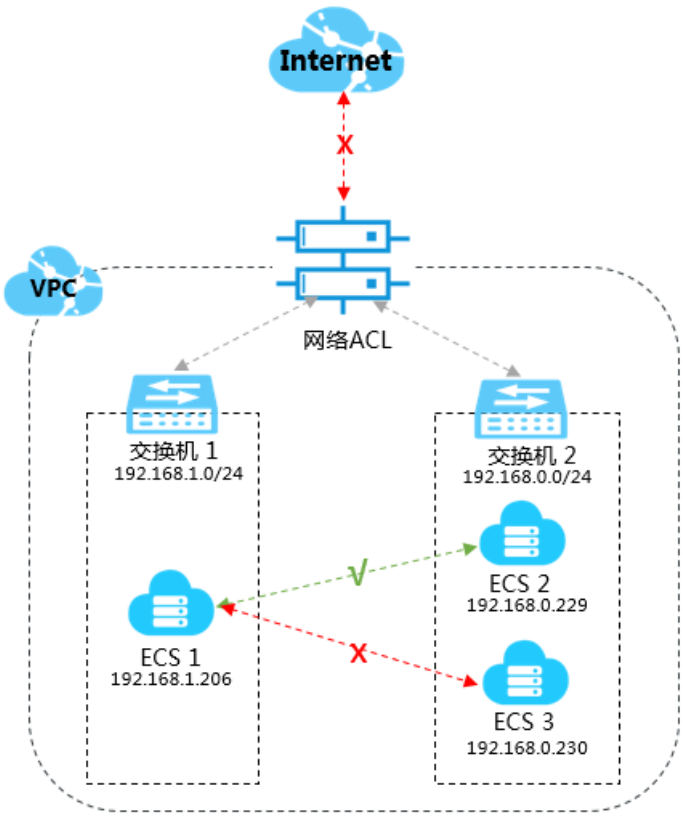
开始前，请确保满足以下条件：

- 您已经创建了专有网络和交换机。具体操作，请参见创建专有网络。
- 您已经在交换机中创建了ECS实例。具体操作，请参见使用向导创建实例。

背景信息

某公司在云上创建了VPC，在VPC中创建了两个交换机，交换机1下创建了ECS1实例（192.168.1.206），交换机2下创建了ECS2实例（192.168.0.229）和ECS3实例（192.168.0.230）。因公司业务需要，要求ECS实例间、ECS与互联网间必须满足以下互通关系。

- 禁止ECS1实例、ECS2实例、ECS3实例与互联网互通。
- 禁止ECS1与ECS3互通。
- 允许ECS1与ECS2互通。



如上图，您可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中ECS流量的访问控制。

配置流程图如下：

步骤一：创建网络ACL

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，单击**创建网络ACL**。
5. 在**创建网络ACL**对话框中，根据以下信息配置网络ACL，然后单击**确定**。
   - **专有网络**：选择网络ACL所属的专有网络。
   - **名称**：输入网络ACL的名称。

     名称长度为2~128个字符，以英文字母或中文开头，可包含数字、下划线（_）和短划线（-）。
   - **描述**：输入网络ACL的描述。

     描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

步骤二：绑定交换机

将交换机1和交换机2绑定到网络ACL。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击网络ACL的ID。
5. 在**已绑定资源**页签下，单击**关联交换机**。
6. 在**关联交换机**对话框，选择交换机1和交换机2，然后单击**确定关联**。

步骤三：添加网络ACL规则

为网络ACL添加入方向规则和出方向规则。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**设置入方向规则**。
5. 在**入方向规则**页签下，单击**管理入方向规则**。
6. 在**管理入方向规则**对话框，根据以下信息配置入方向规则，然后单击**确定**。

优先级	规则名称	策略	协议类型	源地址	源端口范围

优先级	规则名称	策略	协议类型	源地址	源端口范围
1	允许来自ECS2的流量	允许	ALL	192.168.0.229/32	-1/-1
2	允许来自ECS1的流量	允许	ALL	192.168.1.206/32	-1/-1
3	拒绝来自所有地址的流量	拒绝	ALL	0.0.0.0/0	-1/-1

7. 单击**出方向规则**页签，然后单击**管理出方向规则**。
8. 在**管理出方向规则**对话框，根据以下信息配置出方向规则，然后单击**确定**。

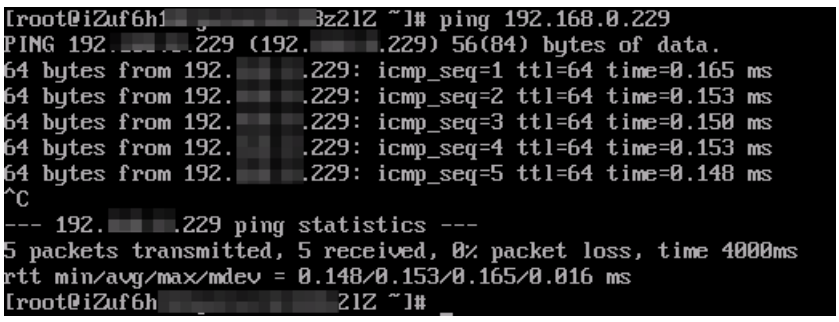
优先级	规则名称	策略	协议类型	源地址	源端口范围
1	允许去往ECS2的流量	允许	ALL	192.168.0.229/32	-1/-1
2	允许去往ECS1的流量	允许	ALL	192.168.1.206/32	-1/-1
3	拒绝去往所有地址的流量	拒绝	ALL	0.0.0.0/0	-1/-1

步骤四：测试连通性

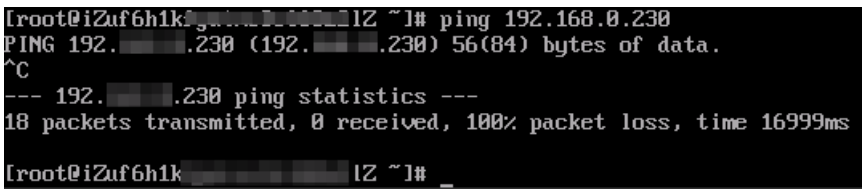
测试ECS间、ECS与互联网间的连通性。

1. 登录ECS1实例。
2. 通过 `ping` 命令分别 `ping` ECS2实例、ECS3实例、任意公网IP地址，验证通信是否正常。经验证，ECS1实例能访问ECS2实例，但不能访问ECS3实例和互联网。

ECS1实例能访问ECS2实例



ECS1实例不能访问ECS3实例



ECS1实例不能访问互联网

```
[root@iZuf[redacted]?lZ ~]# ping 114.[redacted]114
PING 114.[redacted].114 (114.[redacted].114) 56(84) bytes of data.
^C
--- 114.[redacted].114 ping statistics ---
32 packets transmitted, 0 received, 100% packet loss, time 30999ms

[root@iZu[redacted]Z ~]#
```

8.2. 限制本地数据中心与云上的互通

本文为您介绍如何通过网络ACL功能限制本地数据中心与云上的互通关系。

前提条件

开始操作前，请确保满足以下条件：

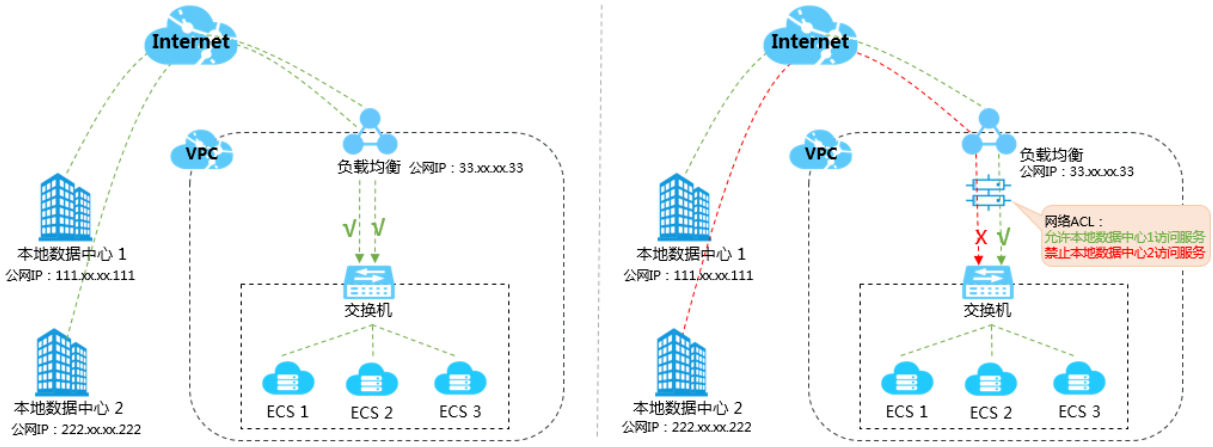
- 您已经创建了专有网络和交换机。具体操作，请参见创建专有网络。
- 您已经在交换机中创建了ECS实例。具体操作，请参见使用向导创建实例。
- ECS实例加入的安全组允许互联网访问ECS实例的HTTP服务。更多信息，请参见安全组应用案例ECS安全组配置操作指南中的案例八。

背景信息

某公司在云上创建了公网负载均衡实例和ECS实例，ECS实例部署了静态网页，负载均衡实例配置了监听并添加ECS实例作为后端服务器。默认情况下，本地数据中心1和本地数据中心2均可以通过负载均衡实例的公网IP地址访问静态网页。因公司业务需要，要求只允许本地数据中心1访问静态网页，禁止本地数据中心2访问静态网页。

各网络的公网IP地址如下表所示：

网络	公网IP地址
本地数据中心1	111.xx.xx.111
本地数据中心2	222.xx.xx.222
负载均衡实例	33.xx.xx.33



如上图，您可以将网络ACL与ECS实例所属的交换机绑定，然后通过配置网络ACL规则实现对交换机中ECS流量的访问控制。

配置流程图如下：

步骤一：创建网络ACL

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，单击**创建网络ACL**。
5. 在**创建网络ACL**对话框中，根据以下信息配置网络ACL，然后单击**确定**。
   - **专有网络**：选择网络ACL所属的专有网络。
   - **名称**：输入网络ACL的名称。

     名称长度为2~128个字符，以英文字母或中文开头，可包含数字、下划线（_）和短划线（-）。
   - **描述**：输入网络ACL的描述。

     描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

步骤二：绑定交换机

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击网络ACL的ID。
5. 在**已绑定资源**页签下，单击**关联交换机**。
6. 在**关联交换机**对话框，选择交换机，然后单击**确定**。

步骤三：添加网络ACL规则

为网络ACL添加入方向规则和出方向规则。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**网络ACL**。
3. 在顶部菜单栏处，选择网络ACL的地域。
4. 在**网络ACL**页面，找到目标网络ACL，单击**操作**列下的**设置入方向规则**。
5. 在**设置入方向规则**页签下，单击**管理入方向规则**。
6. 在**管理入方向规则**对话框，根据以下信息配置入方向规则，然后单击**确定**。

优先级	规则名称	策略	协议类型	源地址	源端口范围
1	允许来自本地数据中心1的HTTP请求	允许	TCP	本地数据中心1的公网IP地址，本示例输入111.xx.xx.111。	80/80

优先级	规则名称	策略	协议类型	源地址	源端口范围
3	拒绝来自本地数据中心2的HTTP请求	拒绝	TCP	本地数据中心2的公网IP地址，本示例输入222.xx.xx.222。	80/80

如果负载均衡实例开启了健康检查功能，您还需添加以下入方向规则。

优先级	规则名称	策略	协议类型	源地址	源端口范围
2	允许健康检查	允许	ALL	负载均衡健康检查使用的地址段，为固定地址段100.64.0.0/10。	-1/-1

7. 单击**出方向规则**页签，然后单击**管理出方向规则**。
8. 在**管理出方向规则**对话框，根据以下信息配置出方向规则，然后单击**确定**。

优先级	规则名称	策略	协议类型	源地址	源端口范围
1	允许去往本地数据中心1的HTTP流量	允许	TCP	本地数据中心1的公网IP地址，本示例输入111.xx.xx.111。	80/80
3	拒绝去往本地数据中心2的HTTP流量	拒绝	TCP	本地数据中心2的公网IP地址，本示例输入222.xx.xx.222。	80/80

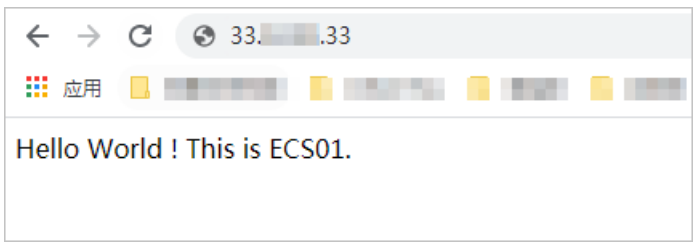
如果负载均衡实例开启了健康检查功能，您还需添加以下出方向规则。

优先级	规则名称	策略	协议类型	源地址	源端口范围
2	允许健康检查	允许	ALL	负载均衡健康检查使用的地址段，为固定地址段100.64.0.0/10。	-1/-1

步骤四：测试连通性

测试本地数据中心1、本地数据中心2与负载均衡实例间的连通性。

1. 在本地数据中心1下，打开PC端的浏览器。
2. 在浏览器中输入 `http://33.xx.xx.33` ，验证通信是否正常。经验证，本地数据中心1下的PC可以访问ECS实例的静态网页。



3. 在本地数据中心2下，打开PC端的浏览器。
4. 在浏览器中输入 `http://33.xx.xx.33` ，验证通信是否正常。经验证，本地数据中心2下的PC不可以访问ECS实例的静态网页。