解决方案实践

基于 JumpServer 快速搭建远程安全运维环境

文档版本 1.0

发布日期 2024-04-22

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

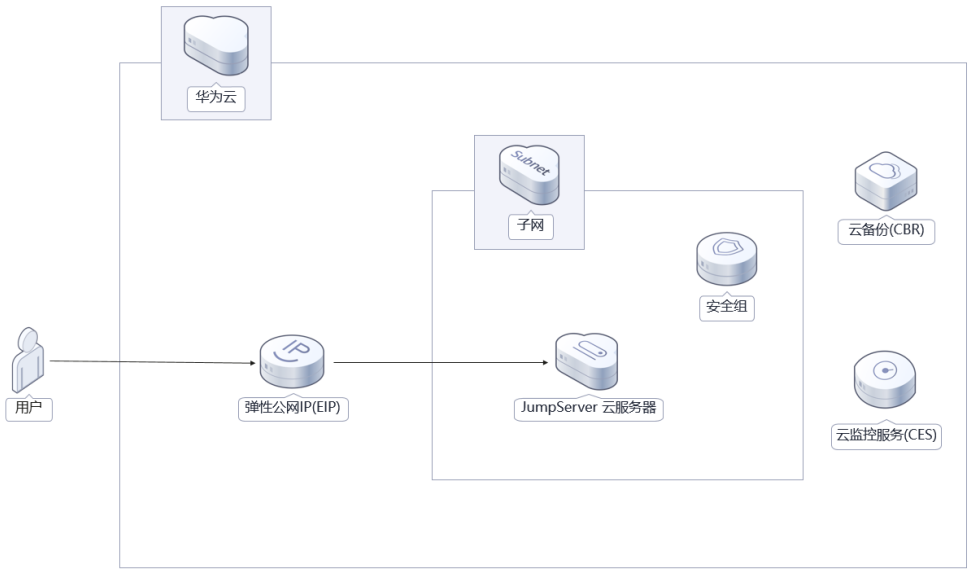
应用场景

该解决方案可以帮助您在华为云弹性云服务器 ECS上基于JumpServer快速搭建远程安全运维环境。为企业提供一种高效、可靠、安全的方式来管理基础设施和应用程序。可应用于金融、制造、服务，互联网等行业，适用于各种需要对服务器进行安全管控的场景。

方案架构

该解决方案在华为云弹性云服务器 ECS上基于JumpServer一键部署快速搭建远程安全运维环境。该解决方案部署架构如下图所示：

图 1-1 方案架构



部署该方案中需要使用的资源：

- 创建一台Linux弹性云服务器 ECS，用于安装JumpServer搭建远程安全运维环境

- 创建一个弹性公网IP EIP并绑定到弹性云服务器 ECS，用于提供访问公网和被公网访问能力。
- 创建安全组，通过配置安全组规则，为弹性云服务器提供安全防护。

此外您可以使用云监控服务 CES来监测弹性云服务器运行状态；通过购买云备份 CBR，对弹性云服务器进行数据备份。

方案优势

- 安全性高

  采用多层安全防护机制，包括基于角色的访问控制、审计日志、多因素认证等，可以有效防止恶意攻击和内部人员的不当操作，保障系统的安全性。
- 管理性强

  提供了丰富的管理功能，包括用户管理、资产管理、账号管理、权限管理等，可以方便地对用户进行管理和监控，保证系统的稳定性和可靠性。
- 一键部署

  一键轻松部署，即可实现弹性云服务器 ECS，弹性公网IP EIP 创建及JumpServer云堡垒机系统的安装。

约束与限制

- 该解决方案部署前，需注册华为账号并开通华为云，完成实名认证。如果计费模式选择“包年包月”，请确保账户余额充足以便一键部署资源的时候可以自动支付；或者在一键部署的过程进入费用中心，找到“待支付订单”手动完成支付。
- 如果选用IAM委托权限部署资源，请确保使用的华为账号有IAM的足够权限，具体请参考**创建rf_admin_trust委托（可选）**；如果使用华为主账号或admin用户组下的IAM子账户可不选委托，将采用当前登录用户的权限进行部署。

2 资源和成本规划

该解决方案主要部署如下资源，不同产品的花费仅供参考，实际以收费账单为准，具体请参考华为云**官网价格**：

表 2-1 资源和成本规划（包年包月）

华为云服务	配置示例	每月预估花费
弹性云服务器 ECS	• 区域：亚太-新加坡 • 计费模式：包年包月 • 规格：X86计算 | ECS | s6.xlarge.2 | 4vCPUs | 8GiB • 镜像：CentOS 7.9 64bit • 系统盘：高IO | 100GB • 购买量：1	$76.93 USD
弹性公网IP EIP	• 按需计费：$0.12 USD/EIP/GB • 区域：亚太-新加坡 • 计费模式：按需计费 • 线路：动态BGP • 公网带宽：按流量计费 • 带宽大小：300Mbit/s • 购买量：1	$0.12 USD/GB
合计		76.93 USD + 弹性公网IP EIP 费用

表 2-2 资源和成本规划（按需计费）

华为云服务	配置示例	每月预估花费

弹性云服务器 ECS	• 按需计费：0.78元/小时 • 区域：亚太-新加坡 • 计费模式：包年包月 • 规格：X86计算 | ECS | s6.xlarge.2 | 4vCPUs | 8GiB • 镜像：CentOS 7.9 64bit • 系统盘：高IO | 100GB • 购买时长：1个月 • 购买量：1	$100.80 USD
弹性公网IP EIP	• 区域：亚太-新加坡 • 计费模式：按需计费 • 线路：动态BGP • 公网带宽：按流量计费 • 带宽大小：300Mbit/s • 购买量：1	$0.12 USD/GB
合计		$100.80 USD + 弹性公网IP EIP费用

3 实施步骤

3.1 准备工作

创建 rf_admin_trust 委托（可选）

步骤1 进入华为云官网，打开**控制台管理**界面，鼠标移动至个人账号处，打开“统一身份认证”菜单。

图 3-1 控制台管理界面

图 3-2 统一身份认证菜单

步骤2 进入“委托”菜单，搜索“rf_admin_trust”委托。

图 3-3 委托列表

- 如果委托存在，则不用执行接下来的创建委托的步骤
- 如果委托不存在时执行接下来的步骤创建委托

步骤3 单击步骤2界面中的“创建委托”按钮，在委托名称中输入“rf_admin_trust”，委托类型选择“云服务”，选择“RFS”，单击“下一步”。

图 3-4 创建委托

步骤4 在搜索框中输入“Tenant Administrator”权限，并勾选搜索结果。

图 3-5 选择策略

步骤5 选择“所有资源”，并单击下一步完成配置。

图 3-6 设置授权范围

步骤6 “委托”列表中出现“rf_admin_trust”委托则创建成功。

图 3-7 委托列表

----结束

3.2 快速部署

本章节主要帮助用户快速部署该解决方案。

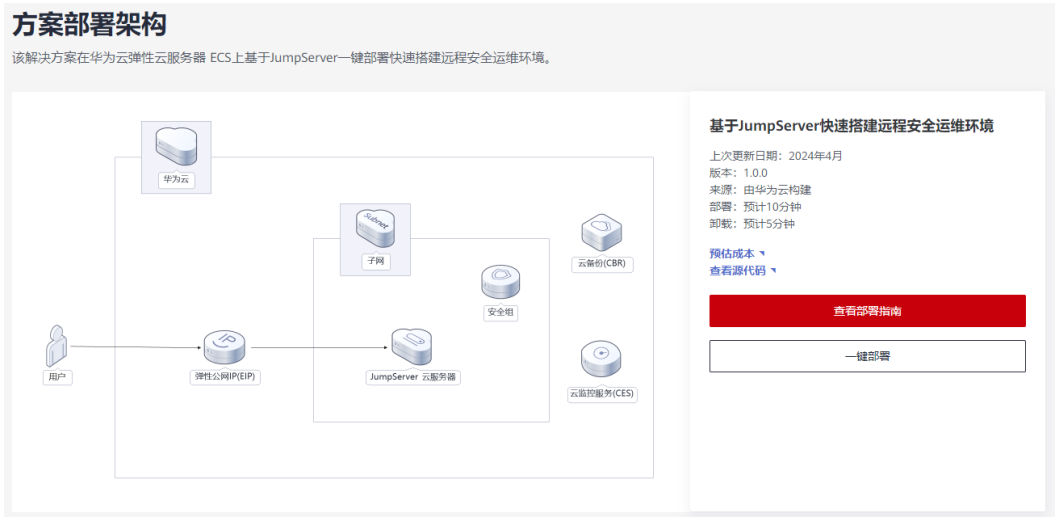
表 3-1 参数填写说明

参数名称	类型	是否必填	参数解释	默认值
vpc_name	String	必填	虚拟私有云名称，该模板使用新建VPC，不允许重名。取值范围：1-54个字符，支持中文、英文字母、数字、_（下划线）、-（中划线）、.（点）。	remote-OM-environment-with-jumpserver-demo
secgroup_name	String	必填	安全组名称，该模板新建安全组，安全组规则请参考**安全组规则修改（可选）**进行配置。取值范围：1-64个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	remote-OM-environment-with-jumpserver-demo
ecs_name	String	必填	弹性云服务器名称，不支持重名。取值范围：1-60个字符，支持中文、英文字母、数字、_（下划线）、-（中划线）、.（点）。	remote-OM-environment-with-jumpserver-demo
ecs_flavor	String	必填	弹性云服务器规格名称，具体请参考官网**弹性云服务器规格清单**。	s6.xlarge.2
ecs_password	String	必填	弹性云服务器初始化密码。取值范围：长度为8-26个字符，密码至少包含大写字母、小写字母、数字和特殊字符（!@$%^-_=+[{()}]:,./?~#*）中的三种，Windows系统密码不能包含用户名或用户名的逆序，不能包含用户名中超过两个连续字符的部分。管理员账户默认root。	空

参数名称	类型	是否必填	参数解释	默认值
ecs_disk_size	Number	必填	弹性云服务器系统盘大小，磁盘类型默认高IO，单位：GB，取值范围为40-1,024，不支持缩盘。	100
bandwidth_size	Number	必填	弹性公网带宽大小，该模板计费方式为按流量计费。单位：Mbit/s，取值范围：1-300 。	300
charging_mode	String	必填	计费模式，默认自动扣费，取值为prePaid（包年包月）或postPaid（按需计费），	postPaid
charging_unit	String	必填	弹性云服务器ECS订购周期类型，仅当charging_mode为prePaid（包年/包月）生效，此时该参数为必填参数。取值范围：month（月），year（年）。	month
charging_period	Number	必填	弹性云服务器ECS订购周期，仅当charging_mode为prePaid（包年/包月）生效，此时该参数为必填参数。取值范围：charging_unit=month（周期类型为月）时，取值为1-9；charging_unit=year（周期类型为年）时，取值为1-3。默认订购1月。	1

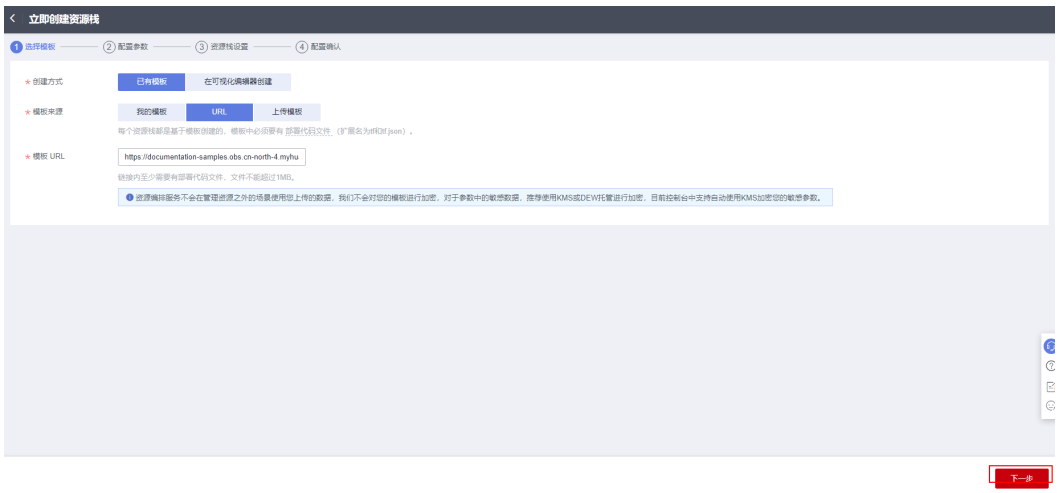
步骤1 登录**华为云解决方案实践**，选择“基于JumpServer快速搭建远程安全运维环境”解决方案。单击“一键部署”，跳转至解决方案创建堆栈界面。

图 3-8 解决方案实施库



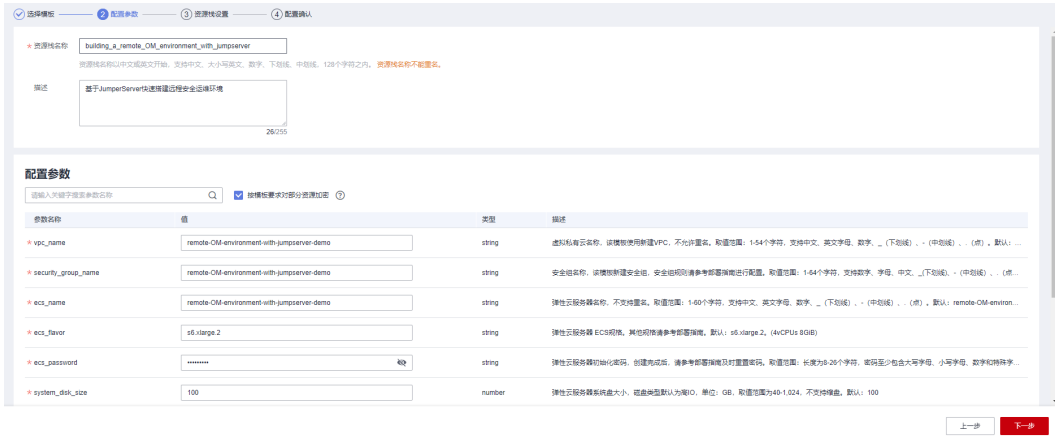
步骤2 在选择模板界面中，单击“下一步”。

图 3-9 选择模板



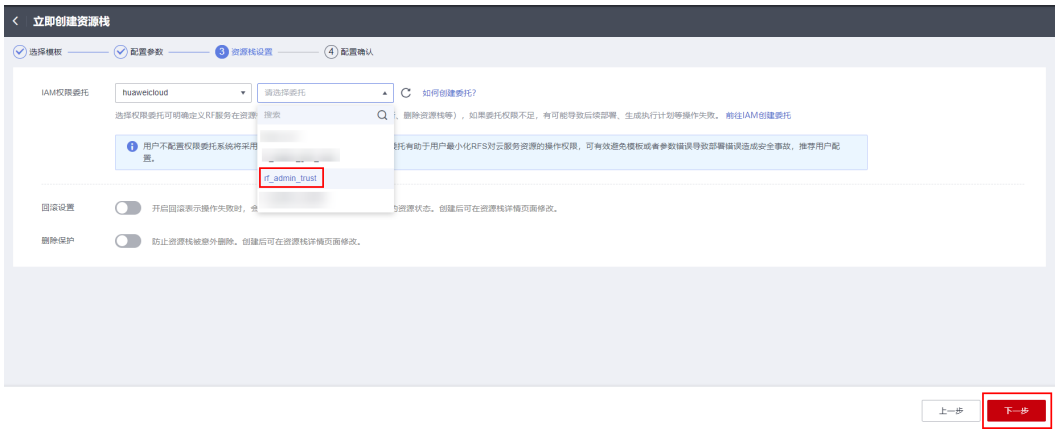
步骤3 在配置参数界面中，参考表3-1完成自定义参数填写，单击“下一步”。

图 3-10 配置参数



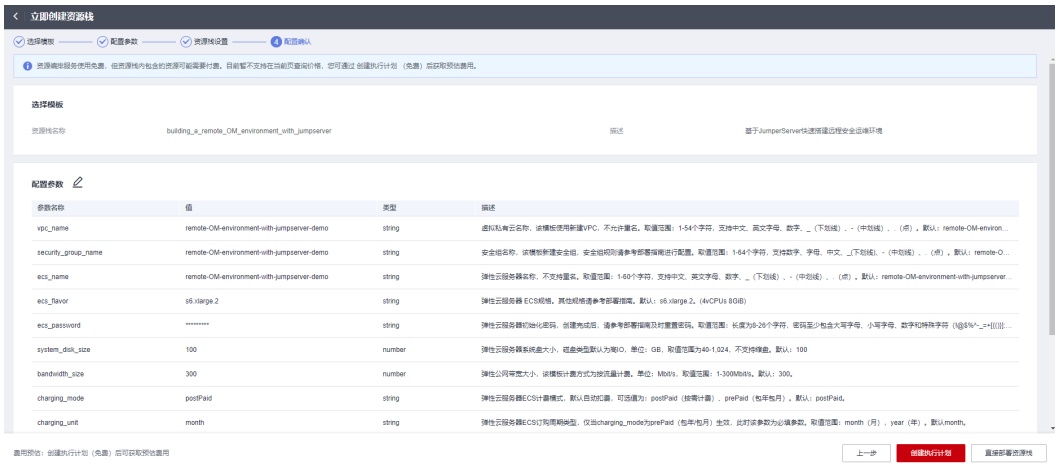
步骤4 （可选，如果使用华为账号或admin用户组下的IAM子账户可不选委托）在资源设置界面中，在权限委托下拉框中选择“rf_admin_trust”委托，单击“下一步”。

图 3-11 资源栈设置



步骤5 在配置确认页面中，单击“创建执行计划”。

图 3-12 配置确认



步骤6 在弹出的创建执行计划框中，自定义填写执行计划名称，单击“确定”。

图 3-13 创建执行计划

步骤7 待执行计划状态为“创建成功，待部署”后，单击“部署”，并且在弹出的执行计划确认框中单击“执行”。

图 3-14 执行计划

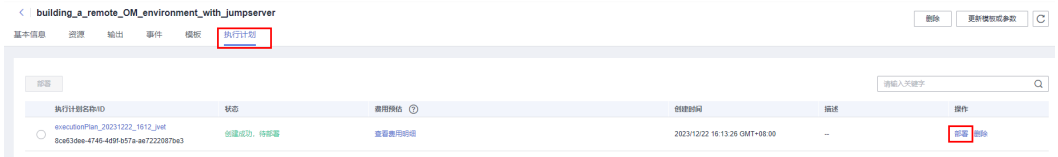
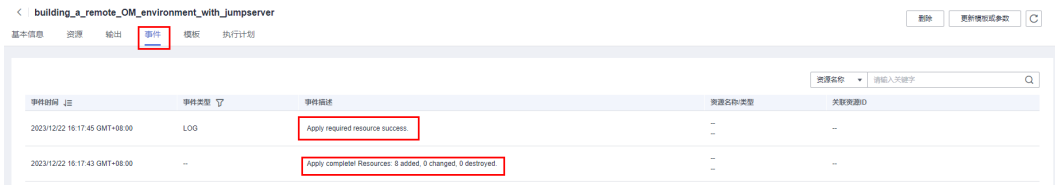


图 3-15 执行计划确认

步骤8 （可选）如果计费模式选择“包年包月”，在余额不充足的情况下（所需总费用请参考**表2-1**）请及时登录费用中心，手动完成待支付订单的费用支付。

步骤9 等待解决方案自动部署。部署成功后，单击“事件”，回显结果如下:

图 3-16 资源创建成功



步骤10 刷新页面，在“输出”中查看JumpServer访问说明。

图 3-17 说明

----结束

3.3 开始使用

安全组规则修改（可选）

安全组实际是网络流量访问策略，包括网络流量入方向规则和出方向规则，通过这些规则为安全组内具有相同保护需求并且相互信任的云服务器、云容器、云数据库等实例提供安全保护。

如果您的实例关联的安全组策略无法满足使用需求，比如需要添加、修改、删除某个TCP端口，请参考以下内容进行修改。

- 添加安全组规则：根据业务使用需求需要开放某个TCP端口，请参考**添加安全组规则**添加入方向规则，打开指定的TCP端口。
- 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。您可以参考**修改安全组规则**，来修改安全组中不合理的规则，保证云服务器等实例的网络安全。
- 删除安全组规则：当安全组规则入方向、出方向源地址/目的地址有变化时，或者不需要开放某个端口时，您可以参考**删除安全组规则**进行安全组规则删除。

须知

按默认参数本方案初始化的部署时间约为10分钟，受弹性云服务器 ECS规格 及弹性公网IP EIP带宽大小等因素影响会有波动。

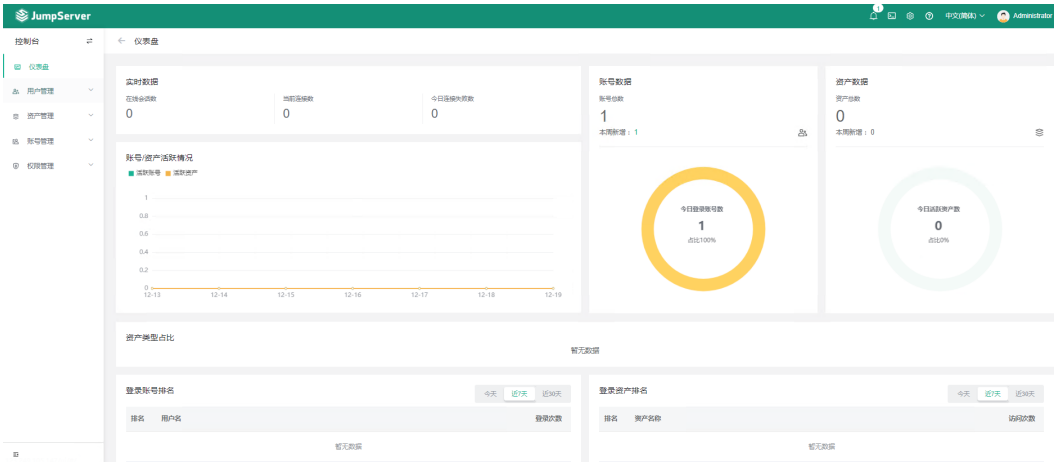
步骤1 登录JumpServer界面。打开浏览器，输入**3.2 快速部署 步骤10**中的访问网址，即可进入JumpServer登录界面，输入用户名和密码单击“登录”（初始用户名：admin，初始密码：admin）

图 3-18 登录界面

步骤2 重置密码，进入管理界面。按照提示，输入新密码，重新输入确认密码，单击“设置”重新使用新密码登录后，即可进入JumpServer控制台界面

图 3-19 重置密码

图 3-20 JumpServer 控制台界面



步骤3 进入JumpServer文档界面。鼠标悬停在右上角如图所示位置，单击“文档”进入JumpServer文档界面，了解更多JumpServer信息。

图 3-21 查看文档

图 3-22 JumpServer 文档界面

----结束

3.4 快速卸载

步骤1 解决方案部署成功后，登录**资源编排服务 RFS**，进入“资源栈”，选择创建的资源栈名称，单击该方案堆栈后的“删除”。

图 3-23 一键卸载

步骤2 在弹出的删除堆栈确认框中，删除方式选择“删除资源”，输入“Delete”，单击“确定”，即可卸载解决方案。

图 3-24 删除堆栈确认

----结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- 弹性云服务器 ECS：是一种可随时自助获取、可弹性伸缩的云服务器，可帮助您打造可靠、安全、灵活、高效的应用环境，确保服务持久稳定运行，提升运维效率。
- 弹性公网IP EIP：提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟VIP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。
- 虚拟私有云 VPC：是用户在云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性IP搭建业务系统。
- 安全组：安全组是一个逻辑上的分组，为同一个VPC内具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当弹性云服务器加入该安全组后，即受到这些访问规则的保护。

5 修订记录

发布日期	修订记录
2023-12-30	第一次正式发布。