解决方案实践

企业云上办公桌面解决方案

文档版本 1.1.0

发布日期 2023-03-07

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 1
2 资源和成本规划 3
3 实施步骤 5
3.1 准备工作 5
3.2 快速部署 14
3.3 开始使用 21
3.4 快速卸载 25
4 附录 26
5 修订记录 27

1 方案概述

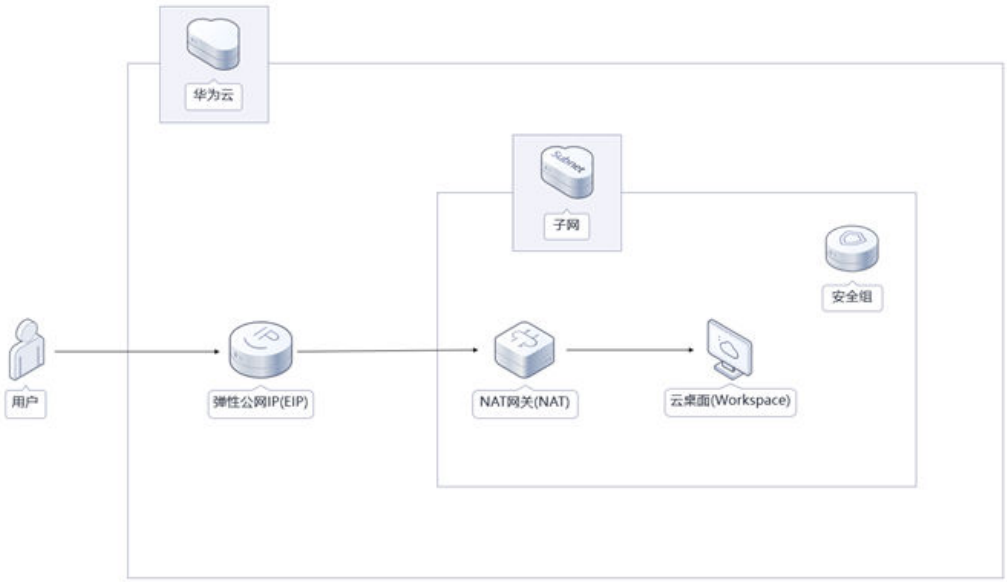
应用场景

该解决方案基于华为云云桌面 Workspace、NAT网关 NAT、弹性公网IP EIP服务，可以帮助您快速部署云上办公空间，构建可靠、安全、灵活、高效的办公环境。

方案架构

此解决方案基于华为云云桌面 Workspace、NAT网关 NAT、弹性公网IP EIP服务，提供一站式企业云上办公服务。该解决方案部署架构如下图所示：

图 1-1 方案架构



该解决方案会部署如下资源：

- 创建一个公网NAT网关 NAT，配置SNAT规则，提供节点访问公网的单向能力，保障数据库环境的访问安全同时方便运维。
- 创建一个弹性公网IP EIP并与NAT网关 NAT绑定，用于提供访问公网的能力。

- 创建云桌面 Workspace，企业无须投入大量的资金和花费数天的部署时间，即可快速构建桌面办公环境。

方案优势

- 体验极致

  自研HDP高清传输协议，真彩无损显示，高清流畅体验，桌面操控延时无感知。

- 安全可靠

  端到端安全防护，数据不落地。安全策略强管控，芯片级安全加密存储。

- 一键部署

  一键轻松部署，即可完成资源的快速发放，企业云上办公桌面环境的部署。

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，且账号不能处于欠费或冻结状态。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”并手动完成支付。
- 确保租户配额充足，在“资源 > 我的配额”中查看配额是否充足，如配额不够，请提前工单申请增加配额。
- 该解决方案会自动进行云桌面租户配置，如果您已经完成租户配置，请前往**云桌面 租户配置**页面删除。
- 该解决方案部署完成后，需用户依据邮件内容指示修改云桌面密码，详**3.3 开始使用**步骤。

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
云桌面 Workspace	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：X86桌面 | 尊享版 | 2vCPUs | 4GiB • 系统盘：高IO | 100GB • 购买量：1	213.00元
弹性公网IP EIP	• 区域：华北-北京四 • 计费模式：包年包月 • 线路：动态BGP • 计费方式：按带宽计费 • 带宽大小：5Mbit/s • 购买时长：1个月 • 购买量：1	115.00元
公网NAT网关	• 区域：华北-北京四 • 规格：小型 • 购买时长：1个月 • 购买量：1	306.00元
合计		634.00元

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
云桌面 Workspace	• 区域：华北-北京四 • 计费模式：按需计费 • 规格：X86桌面 | 尊享版 | 2vCPUs | 4GiB • 系统盘：高IO | 100GB • 购买量：1	0.68 * 24 * 30 = 489.60元
弹性公网IP EIP	• 区域：华北-北京四 • 计费模式：按需计费 • 线路：动态BGP • 计费方式：按带宽计费 • 带宽大小：5Mbit/s • 购买时长：1个月 • 购买量：1	0.34 * 24 * 30 = 244.80元
公网NAT网关	• 区域：华北-北京四 • 规格：小型 • 购买时长：1天 • 购买量：1	12*30=360元
合计		1094.40元

3 实施步骤

3.1 准备工作
3.2 快速部署
3.3 开始使用
3.4 快速卸载

3.1 准备工作

创建 rf_amdin_trust 委托

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”，选择“普通账号”，委托的账号，输入“op_svc_IAC”，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

创建安全组，购买弹性云服务器（可选，如果部署模板为 AD 域连接，则需执行以下步骤）

步骤1 进入华为云**安全组控制台**，创建安全组，选择自定义模板，填写信息，如下图所示。单击“确定”，弹出窗口单击“配置规则”。

图 3-8 创建安全组

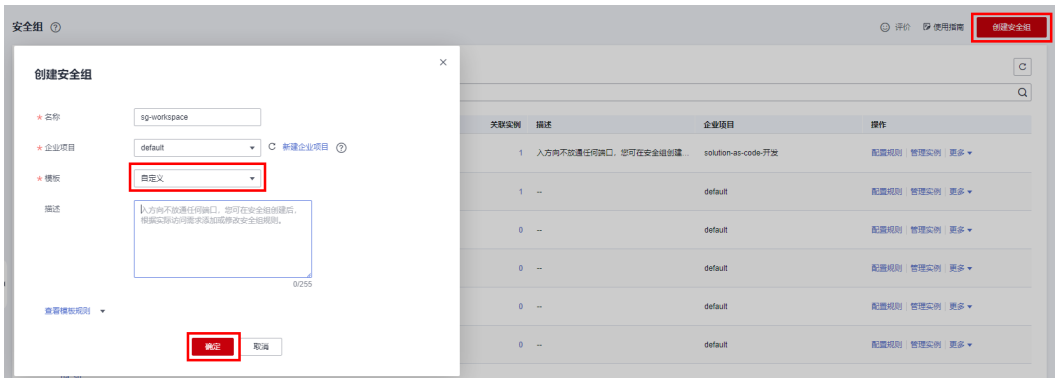


图 3-9 选择配置规则

图 3-10 配置规则

说明

1、安全组入方向规则放通以下端口：

TCP：53,88,135,139,389,445,464,593,636,3268,49152-65535

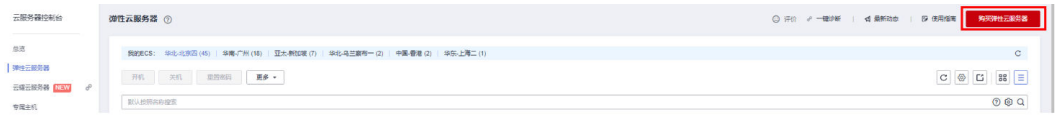
UDP：53,88,123,137,138,389,445,464,500,1024,49152-65535

2、安全组源地址为：

步骤1 AD域服务所属虚拟私有云VPC的网段，例如: 192.168.0.0/16

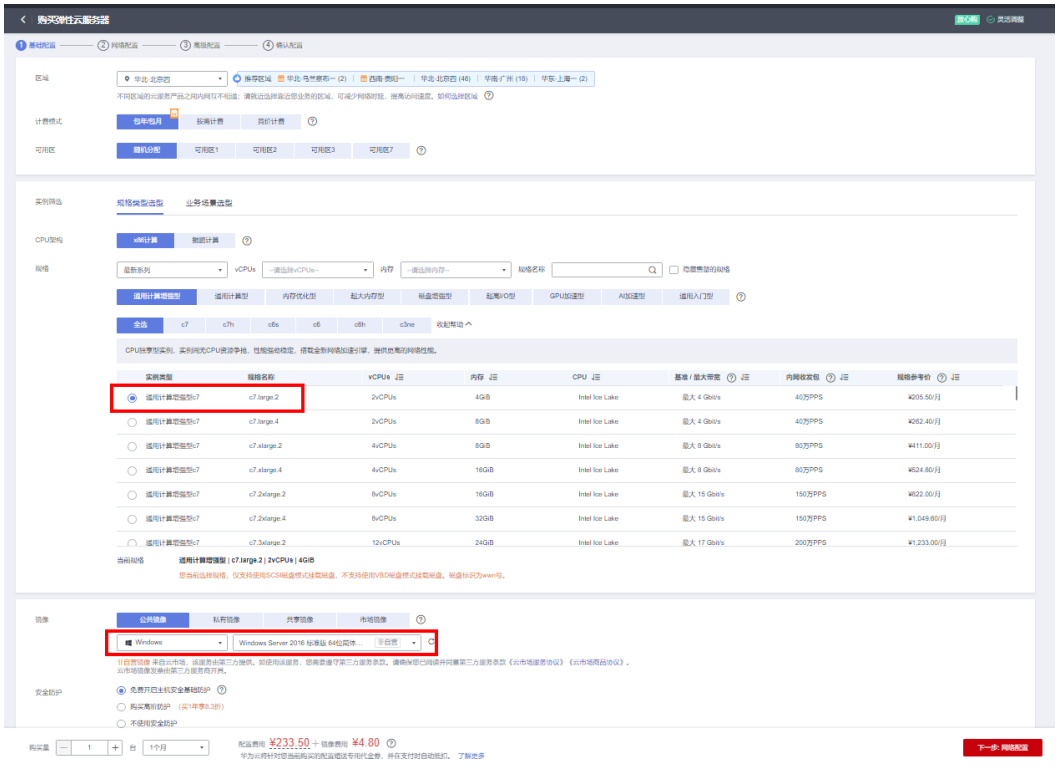
步骤2 进入华为云**弹性云服务器控制台界面**，单击“购买弹性云服务器”。

图 3-11 弹性云服务器控制台界面



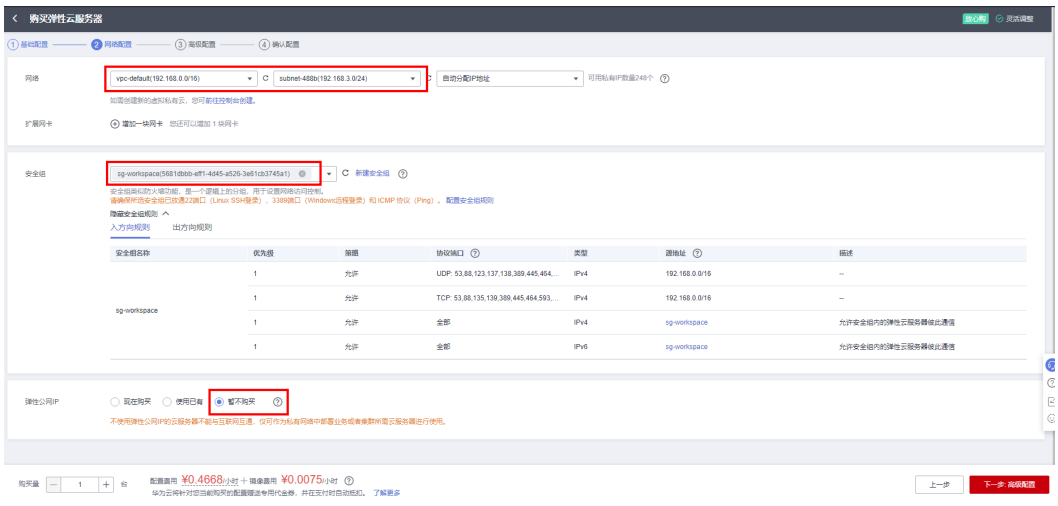
步骤3 选择服务器配置，规格：通用计算型c7 2vCPUs 4GiB 镜像：Windows Server 2016 64位简体中文版 如图9所示，单击“下一步网络配置”。

图 3-12 ECS 基础配置

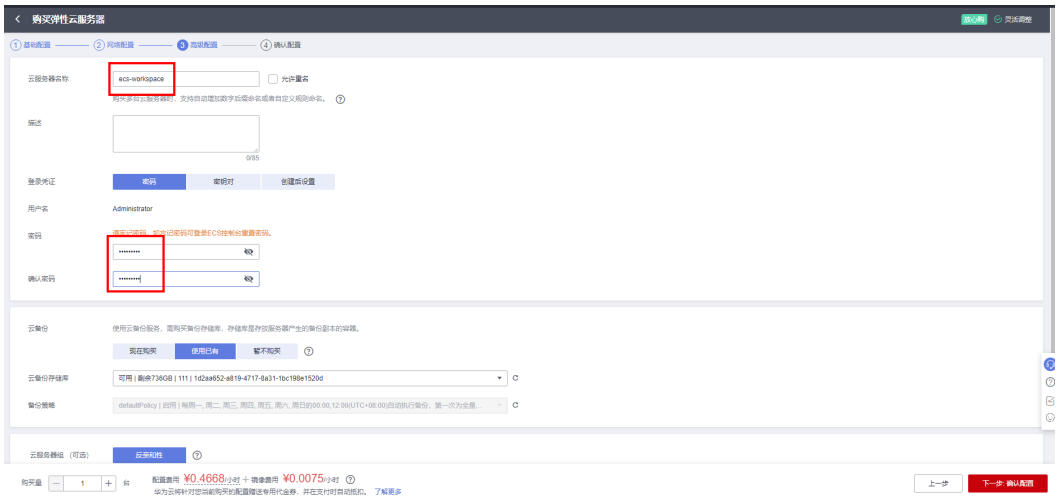


步骤4 进行服务器网络配置，选用已有VPC、子网、（如果没有，请参考**创建虚拟私有云和子网**新建。）及**步骤1**新建的安全组，单击“高级配置”。

图 3-13 网络配置



步骤5 高级配置，填写ECS名称，密码等信息。单击“确认配置”。



----结束

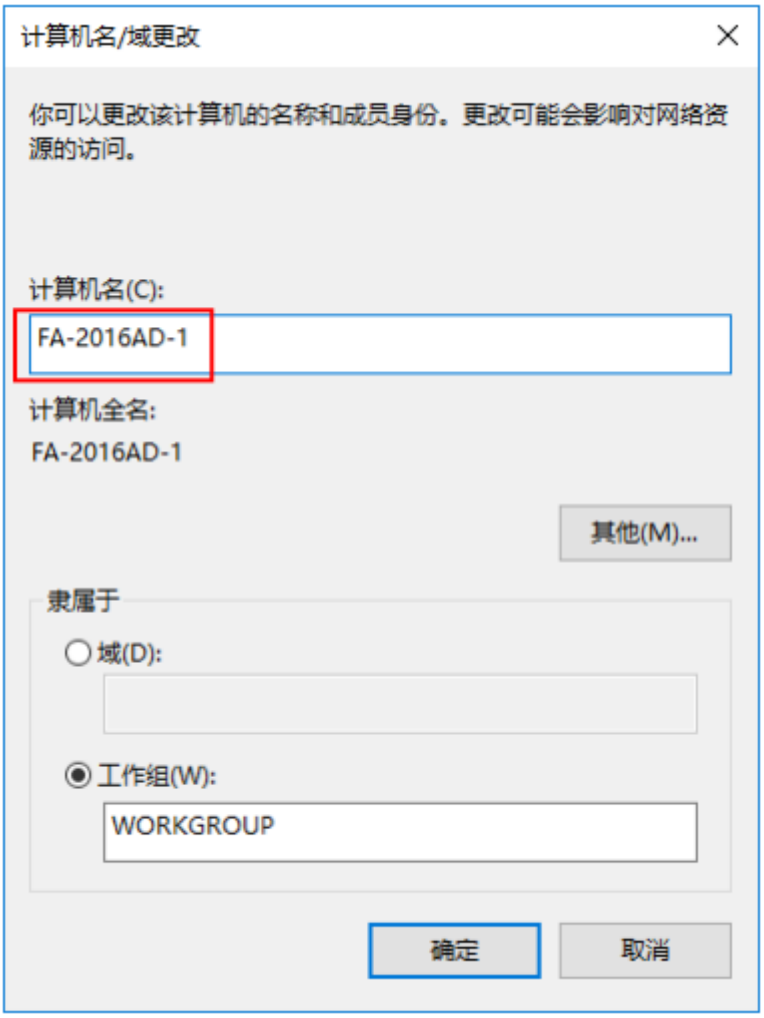
配置 Windows AD 域（可选，如果部署模板为 AD 域连接，则需执行以下步骤）

本章节用于指导用户部署配置Windows AD服务器，用户OU及用户。如果已有，请忽略本章节配置。

步骤1 登录弹性云服务器，在左下角的任务栏，右键单击 ，在“运行”对话框中，输入“sysdm.cpl”，按“Enter”。打开“系统属性”窗口。

步骤2 单击“更改”，在“计算机名”中填入规划的计算机名；单击“确定”，如下图所示。

图 3-14 修改计算机名



步骤3 根据界面提示完成配置，重新启动计算机后使用Administrator账号登录。

步骤4 配置Windows AD域 请参考**如何部署AD服务器**。

步骤5 AD服务器上创建用户OU 请参考**如何在AD服务器上创建用户OU**。

步骤6 AD服务器上创建AD域管理员账户 请参考**如何在AD服务器上创建用户**。

步骤7 AD服务器上创建云桌面用户 请参考**如何在AD服务器上创建用户**（注意：云桌面用户不能和管理员账户相同，请修改文档中登录用户名，部署模板默认为“users_0001”）。

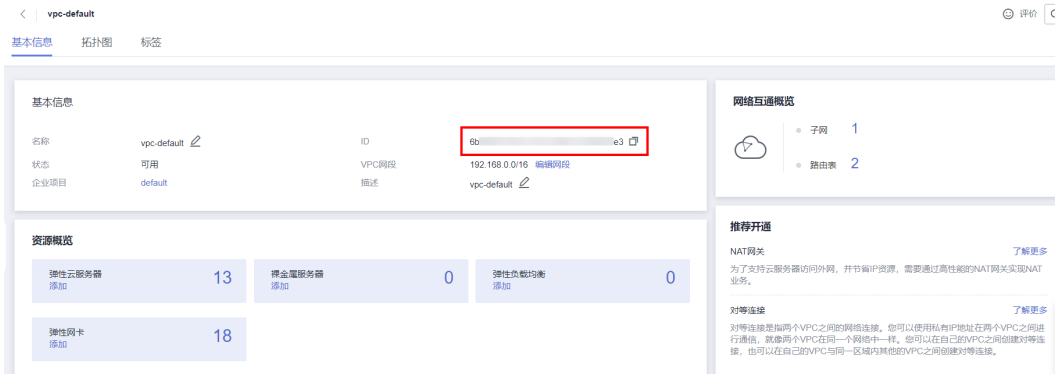
----结束

获取 VPC 及子网 ID

步骤1 登录**华为云官网控制台**，单击**虚拟私有云VPC**，单击AD域服务所属虚拟私有云VPC，获取VPC ID。

图 3-15 虚拟私有云 VPC

图 3-16 VPC ID

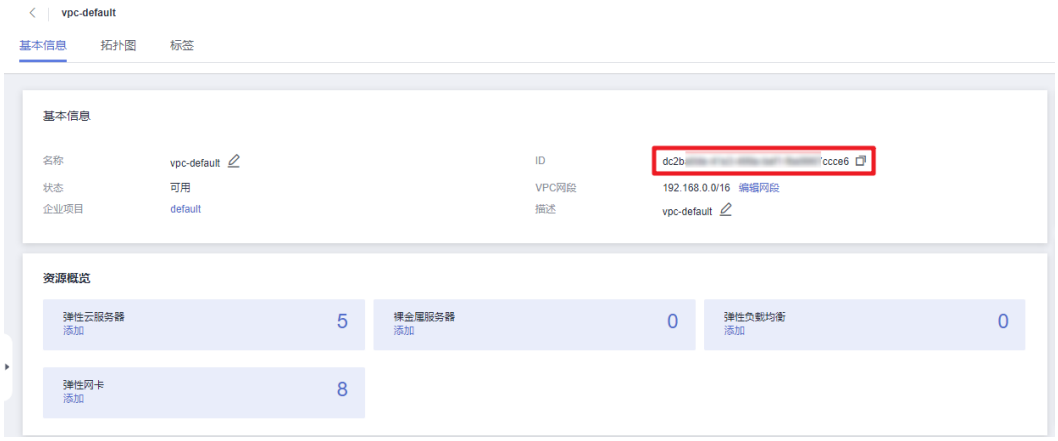


步骤2 打开后端业务服务器所属VPC，单击该VPC下的**子网**，单击任一子网或后端业务服务器所属子网，获取网络ID。

图 3-17 VPC 下的子网

图 3-18 子网列表

图 3-19 子网网络 ID



----结束

获取服务器私有 IP 地址

步骤1 进入华为云**弹性云服务器控制台**，查找到**步骤5**创建的ECS名称，获取IP地址栏下的私有IP地址。

图 3-20 获取服务器私有 IP 地址

----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（本地连接）

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，该模板新建VPC，不允许重名。取值范围：1～54个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	enterprise-cloud-based-office-desktop-demo

参数名称	类型	是否必填	参数解释	默认值
secgroup_name	String	必填	安全组名称，该模板新建安全组，安全组规则请参考部署指南进行配置。取值范围：1～64个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	enterprise-cloud-based-office-desktop-demo
user_name	String	必填	云桌面所属的用户名。取值范围：1～20个字符，支持字母、数字、_(下划线)、-（中划线），必须以字母开头。	desktop-user-demo
image_type	String	必填	云桌面镜像类型，有效值：market（市场镜像）、gold（公有镜像）、private（私有镜像）。	market
flavor_id	String	必填	云桌面 flavor id 请调用 **API Explorer 镜像API** 获取。填写接口响应结果中 product_id 对应的值。	workspace.x86.ultimate.large2
image_id	String	必填	云桌面 image id 请调用 **API Explorer 镜像API** 获取。	空
user_group	String	必填	云桌面所属的用户组，有效值：sudo（Linux 管理员组）、default（Linux 默认用户组）、administrators（Windows 管理员组）、users（Windows 标准用户组）。	administrators
user_email	String	必填	邮箱地址，用于注册云桌面用户。	空
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），默认postPaid。	postPaid
charging_unit	String	必填	有效值为“year”或“month”。当charging_mode（计费模式）为prePaid时，此选项为必填项。	month

参数名称	类型	是否必填	参数解释	默认值
charging_period	number	必填	包年包月时长，当charging_unit取值为“year”,取值范围为1～3；当charging_unit取值为“month”,取值范围为1～9。当charging_mode（计费模式）为prePaid时，此选项为必填项。	1
eip_bandwidth_size	number	必填	弹性公网IP带宽大小，取值范围为1-2000Mbit/s。	5
access_mode	String	必填	云桌面的访问方式，有效值：INTERNET（互联网接入）、DEDICATED（专线接入）、BOTH（支持互联网访问和专用访问）。	INTERNET

表 3-2 参数填写说明（AD 域连接）

参数名称	类型	是否必填	参数解释	默认值
vpc_id	String	必填	虚拟私有云ID，该模板使用已有VPC，请选择AD域服务器所在虚拟私有云VPC，查询VPC请参考**3.1获取VPC、子网、安全组ID步骤1**。	空
subnet_id	String	必填	子网ID，该模板使用已有子网，请选择AD域服务器相同虚拟私有云VPC下子网，查询并获取子网ID请参考**3.1获取VPC、子网、安全组ID步骤2**。	空
user_name	String	必填	云桌面所属的用户名。取值范围：1～20个字符，支持字母、数字、_(下划线)、-（中划线），必须以字母开头。	desktop-user-demo
image_type	String	必填	云桌面镜像类型，有效值：market（市场镜像）、gold（公有镜像）、private（私有镜像）。	market
flavor_id	String	必填	云桌面 flavor id 请调用 **API Explorer 镜像API** 获取。填写接口响应结果中 product_id 对应的值。	workspace.x86.ultimate.large2
image_id	String	必填	云桌面 image id 请调用 **API Explorer 镜像API** 获取。	空

参数名称	类型	是否必填	参数解释	默认值
user_group	String	必填	云桌面所属的用户组，有效值：sudo（Linux 管理员组）、default（Linux 默认用户组）、administrators（Windows 管理员组）、users（Windows 标准用户组）。	administrators
user_email	String	必填	邮箱地址，用于注册云桌面用户。	空
access_mode	String	必填	云桌面的访问方式，有效值：INTERNET（互联网接入）、DEDICATED（专线接入）、BOTH（支持互联网访问和专用访问）。	INTERNET
ad_domain_name	String	必填	Windows AD域名，取值范围：域名用字母（A-Z，a-z，大小写等价）、数字（0-9）和连接符（-）组成，各级域名之间用实点（.）连接，国际域名75个字符。注意连接符（-）不能作为域名的开头或结尾字符。示例：download.game-apk1.com。	vdesktop.huawei.com
ad_server_admin_account	String	必填	域管理员账户。它必须是 AD 服务器上的现有域管理员账户。	JRS0001
ad_server_admin_password	String	必填	域管理员账户密码。它必须是 AD 服务器上的现有域管理员账户密码。	空
ad_master_domain_ip	String	必填	AD服务器私有IP地址，请参考**获取服务器私有IP地址**获取。	空
active_domain_name	String	必填	域控制器名称，由AD服务的主机名加上域名表示。	fa-2016ad-1.vdesktop.huawei.com
charging_mode	String	必填	弹性公网IP计费模式，默认自动扣费，取值为prePaid（包年包月）或postPaid（按需计费），默认postPaid。	postPaid
charging_unit	String	必填	弹性公网IP计费周期，有效值为“year”或“month”。当charging_mode（计费模式）为prePaid时，此选项为必填项。	month

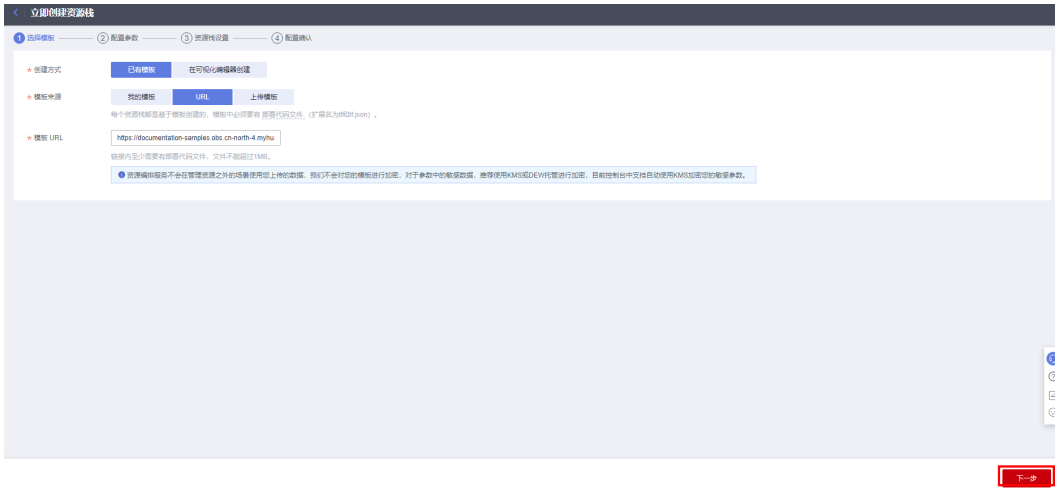
参数名称	类型	是否必填	参数解释	默认值
charging_period	number	必填	弹性公网IP包年包月时长，当charging_unit取值为“year”,取值范围为1～3；当charging_unit取值为“month”,取值范围为1～9。当charging_mode（计费模式）为prePaid时，此选项为必填项。	1
eip_bandwidth_size	number	必填	弹性公网IP带宽大小，以Mbit/s为单位，取值范围为1～2000。	5

步骤1 登录华为云解决方案实践，选择"企业云上办公桌面解决方案"，单击“一键部署”，跳转至解决方案创建资源栈界面。

图 3-21 解决方案实施库

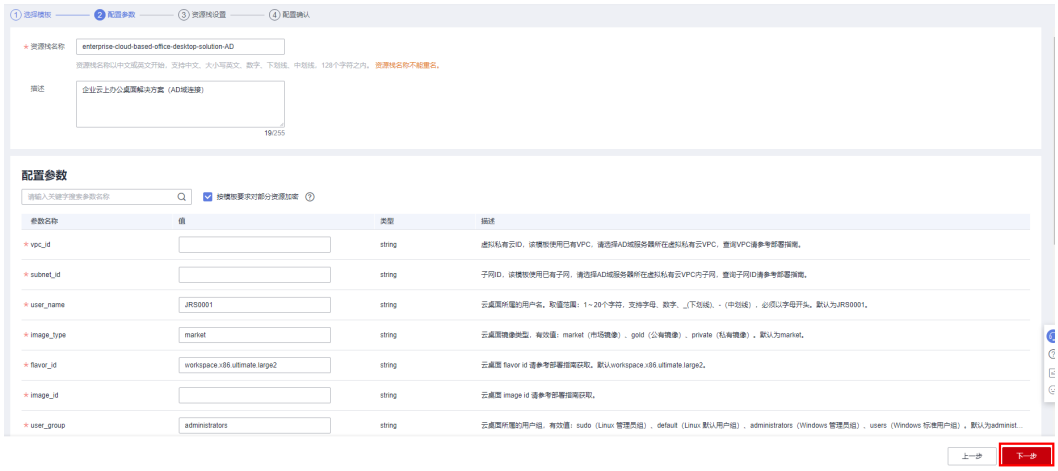
步骤2 在选择模板界面中，单击“下一步”。

图 3-22 选择模板



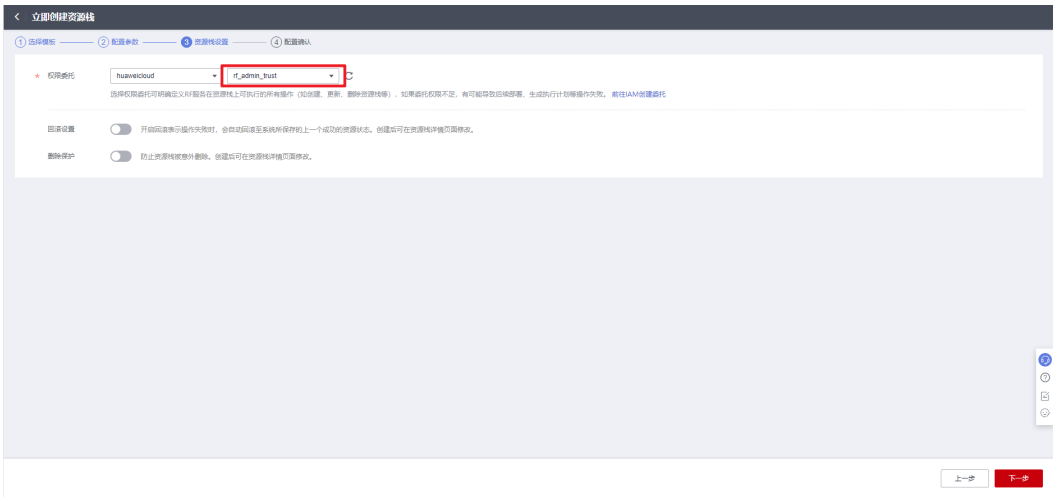
步骤3 在配置参数界面中，参考**表1 参数填写说明（本地连接）**或**表3-2**完成自定义参数填写，单击“下一步”。

图 3-23 配置参数



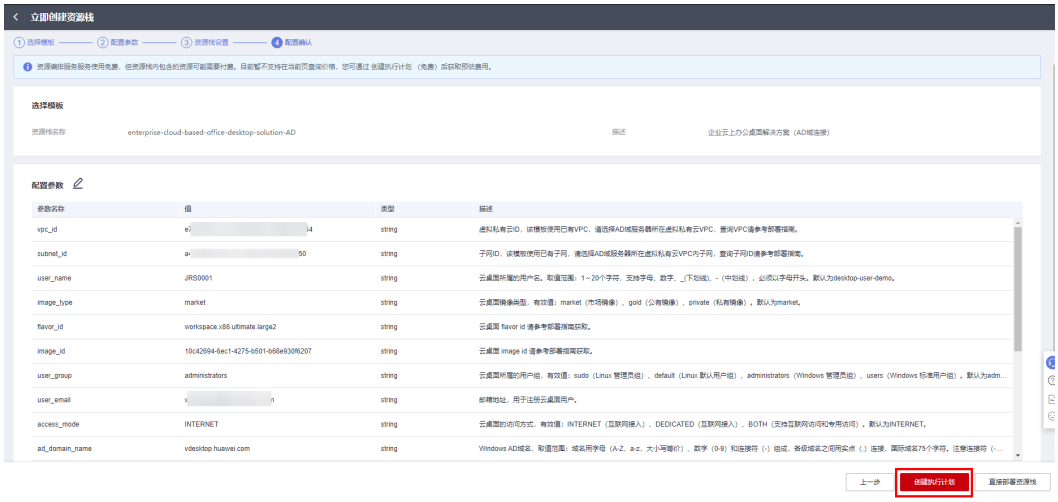
步骤4 在资源设置界面中，在权限委托下拉框中选择“rf_admin_trust”委托，单击“下一步”。

图 3-24 资源栈设置



步骤5 在配置确认界面中，单击“创建执行计划”。

图 3-25 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 3-26 创建执行计划

步骤7 单击“部署”，并且在弹出的执行计划确认框中单击“执行”。

图 3-27 执行计划

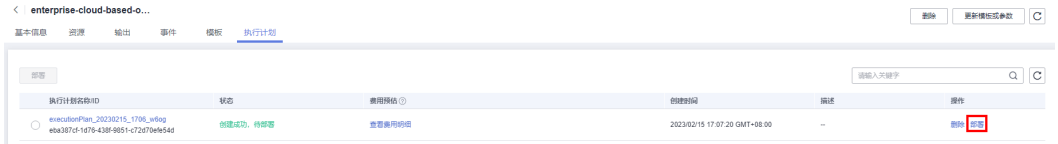


图 3-28 执行计划确认

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 待“事件”中出现“Apply required resource success”，表示该解决方案已经部署完成。

图 3-29 部署完成

----结束

3.3 开始使用

安全组规则修改

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。

云桌面初始化

步骤1 方案部署完成后根据邮箱信息提示，下载客户端并安装。

图 3-30 邮件信息

管理员已为您创建了新的桌面（**DESKTOPUSERDE01**），请按照以下指引完成配置并登录使用吧！

1.客户端下载并安装 前往下载>>

2.服务器设置

接入地址: **https://1 3**

企业ID: **6**

3.用户登录

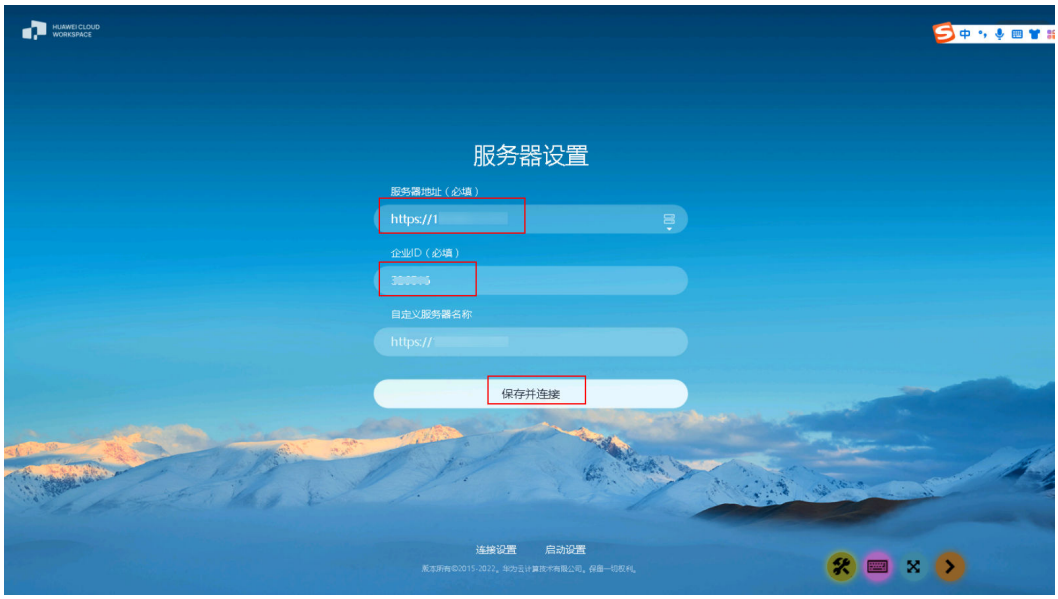
用户名: **desktop-user-demo**

初始密码: **使用您已经设置好的密码**

注意：若忘记密码，可在客户端通过点击忘记密码，或联系管理员重置密码

步骤2 根据邮件信息，填写服务器设置需要的参数。单击“保存并连接”

图 3-31 服务器设置



步骤3 单击“忘记密码”，进行重置密码操作。（如果使用AD域连接，可跳过此步骤，如果需修改密码，请联系AD域服务器管理员。）。

图 3-32 忘记密码

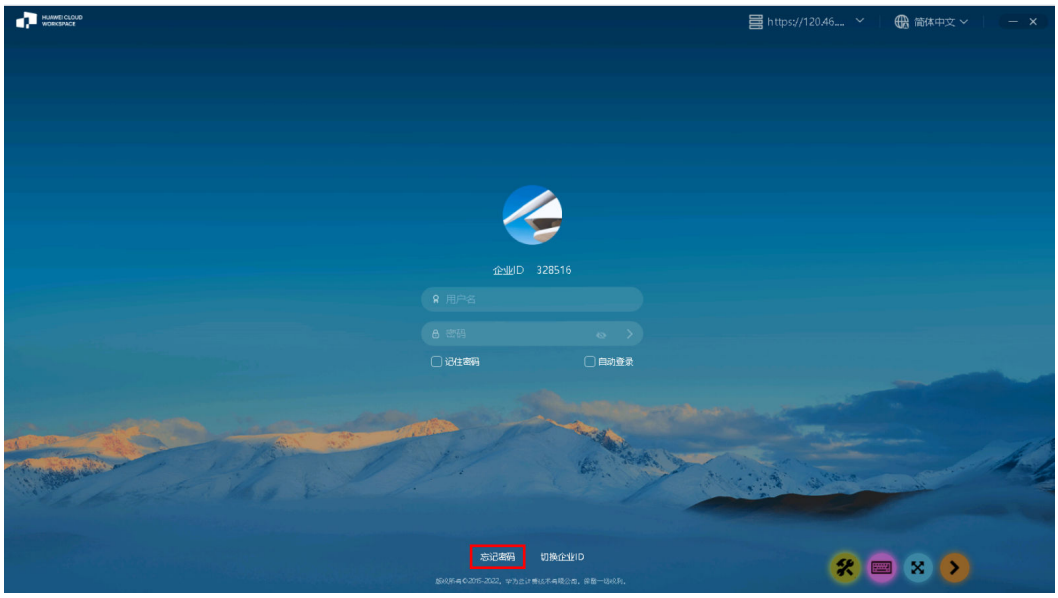


图 3-33 重置密码申请

图 3-34 重置密码

步骤4 输入用户名，密码信息，单击密码框右侧箭头。登录云桌面。

图 3-35 登录云桌面

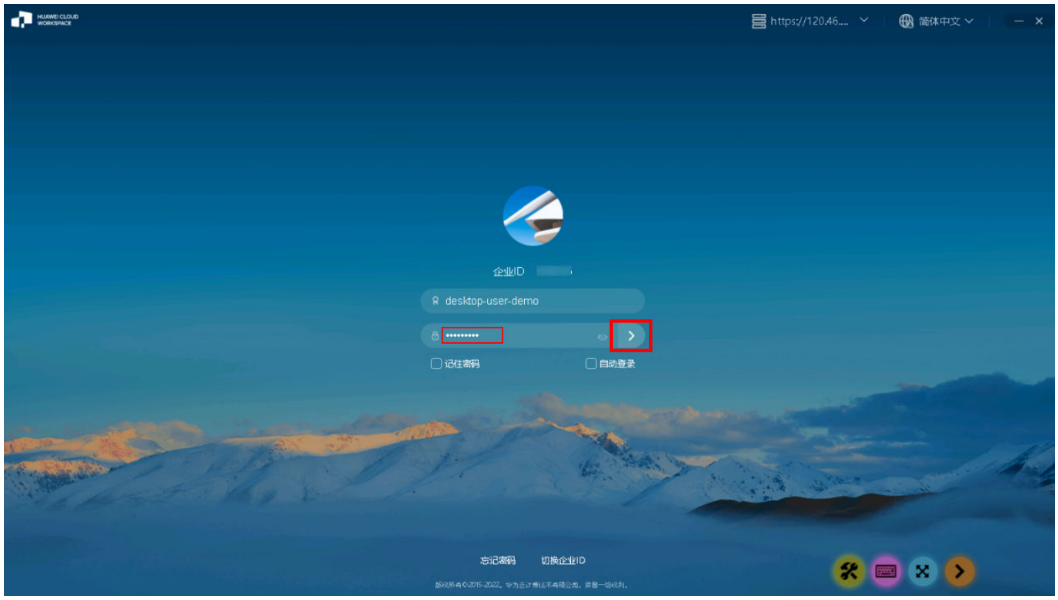
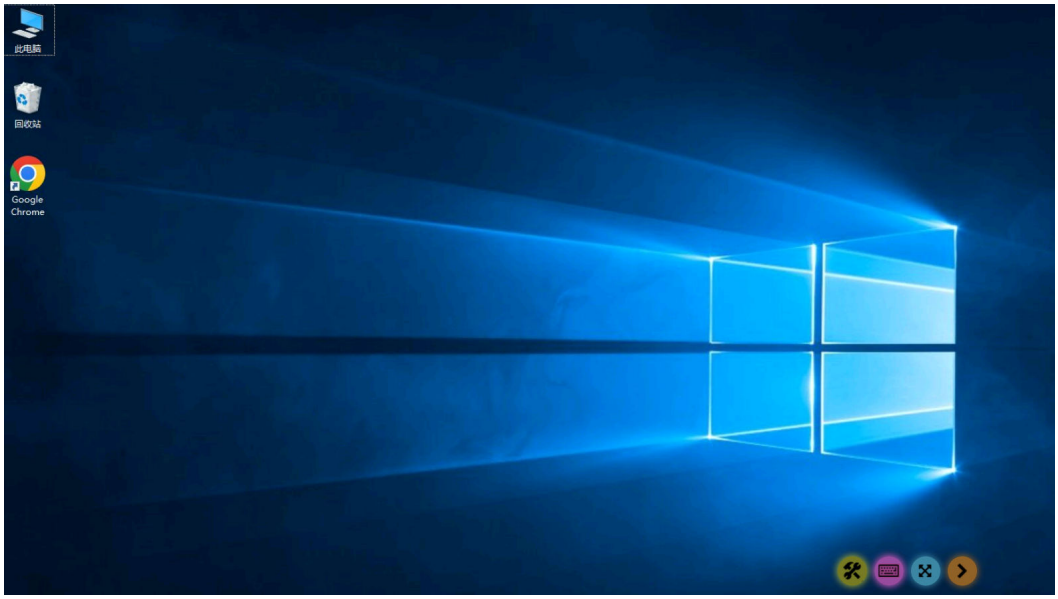


图 3-36 云桌面



----结束

3.4 快速卸载

步骤1 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“删除”。在弹出的删除资源栈确认框中，输入"Delete"，单击“确定”，即可卸载解决方案。

图 3-37 一键卸载

----结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- **云桌面 Workspace**：是一种云上虚拟桌面服务，支持云桌面的快速创建、部署和集中运维管理。无需投入大量的硬件部署，云桌面可按需申请轻松使用，云桌面助您打造更精简、更安全、更低维护成本、更高服务效率的IT办公系统。
- 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IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。
- NAT网关 NAT：支持将私网IP转换为公网IP，转换后，云上资源即可安全地访问公网或对外提供服务，并且保护私有网络信息不直接对公网暴露。

5 修订记录

发布日期	修订记录
2022-12-30	第一次正式发布。
2023-02-28	支持AD域连接。