云堡垒机

快速入门

文档版本 07

发布日期 2024-09-29

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

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 快速购买并登录堡垒机

云堡垒机（Cloud Bastion Host，CBH）是一款统一安全管控平台，为企业提供集中的账号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。

通过购买云堡垒机，使用admin账号添加资源和策略即可实现对资源的运维和审计，同时可通过admin账号创建不同角色进行权限划分管理。

本文以购买10资产量的标准版单机实例类型为例，实现快速对Linux主机资源的运维和审计。

- 购买版本：标准版
- 性能规格：10资产量
- 实例类型：单机
- 纳管资源类型：Linux主机资源

操作流程

本文档介绍如何快速购买、配置云堡垒机。

图 1-1 快速购买配置云堡垒机流程图

表 1-1 购买配置云堡垒机流程说明

步骤	说明
准备工作	使用云服务前，您需要注册华为账号并开通华为云、完成实名认证、为账户充值。
步骤一：购买堡垒机	在云堡垒机控制台购买10资产量的标准版单机实例类型堡垒机。
步骤二：登录堡垒机	购买堡垒机后会使用默认的admin账号登录堡垒机。

步骤	说明
步骤三：添加资源	使用admin在堡垒机添加需要纳管的Linux资源，实现通过堡垒机访问资源，同时也可使用admin账号创建不同角色的账号实现权限的细分管理。
步骤四：添加访问控制策略	使用admin为资源绑定管理角色，同时配置登录的时间段、操作权限、黑名单或白名单等信息，创建对资源的访问控制策略。

准备工作

在购买CBH资源之前，请先注册华为账号并开通华为云、完成实名认证、为账户充值。请保证账户有足够的资金，以免购买资源失败。

1. 注册华为账号并开通华为云，完成实名认证。如果您已有一个华为账号，请跳到下一个任务。

   如果您还没有华为账号，请执行以下操作。

   a. 注册华为账号并开通华为云。

   b. 参考实名认证，完成个人或企业账号实名认证。

2. 为账户充值。您需要确保账户有足够金额，充值方式请参见账户充值。

步骤一：购买堡垒机

步骤1 登录管理控制台。

步骤2 在页面左上角单击  ，选择区域，选择“安全与合规 > 云堡垒机”，进入云堡垒机实例管理页面。

步骤3 单击“购买云堡垒机”，进入云堡垒机的购买页面。

步骤4 选择“云堡垒机实例”服务类型，根据设置实例的相关参数，相关说明请参考表1-2。

表 1-2 购买云堡垒机实例参数说明

参数	示例	说明
计费模式	**包年/包月**	选择实例计费模式，可选择“包年/包月”模式。 包年/包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景。 按需计费：以小时计费。
当前区域	**华东-上海一**	选择堡垒机的使用区域，建议与待管理的ECS、RDS等服务器资源选择同一区域，可以降低网络时延、提高访问速度。

参数	示例	说明
实例类型	**单机**	根据您的自身业务需求选择单机或者主备实例类型。 ● 单机：购买后只有一台堡垒机。 ● 主备：购买后会下发两台堡垒机，组成双机设备，主设备不可正常使用时可继续使用备用堡垒机， **说明** 如您购买的是主备实例，切勿禁用HA，否则会导致对应堡垒机无法登录。
可用分区	**默认即可**	可用区是购买的堡垒机部署的位置。 **说明** 主备实例会将主设备和备用设备分别部署在不同可用区，因此需要分别选择主可用区和备可用区，同样保持默认值即可。
实例名称	**CBH-shanghai-01**	自定义实例名称。
性能规格	**10资产量**	选择实例版本规格。 云堡垒机配备10/20/50/100/200/500/1000/2000/5000/10000资产规格。 资产量表示当前购买的云堡垒机支持的最大可纳管的资源数和最大并发数，同时不同资产量对应的处理器、数据盘、系统盘大小都将会不同，资产量规格详情请参见**服务版本差异**。 示例：选择100资产量表示可纳管资源数和最大并发数都为100个。
版本选择	**标准版**	云堡垒机提供“标准版”和“专业版”两个版本，专业版支持对数据库资源的纳管，版本差异详情请参见**服务版本差异**。
存储扩展包	**0**	如果您有超过资产量对应存储规格时，您可以通过存储扩容包进行扩容，资产量规格详情请参见**服务版本差异**。
虚拟私有云	**vpc-default(192.168.x.x/xx)**	选择当前区域下虚拟私有云（Virtual Private Cloud，VPC）网络。 若当前区域无可选VPC，可单击“查看虚拟私有云”创建新的VPC。 **说明** ● 默认情况下，不同区域的VPC之间内网不互通，同区域的不同VPC内网不互通，同一个VPC下的不同可用区之间内网互通。 ● 云堡垒机支持直接管理同一区域同一VPC网络下ECS等资源，同一区域同一VPC网络下ECS等资源可以直接访问。若需管理同一区域不同VPC网络下ECS等资源，要通过**对等连接**、VPN等打通两个VPC间的网络；不建议跨区域管理ECS等资源。 更多关于VPC网络介绍，请参见**VPC网络规划**。
分配IPv4地址	**自动分配IP地址**	选择“自动分配IP地址”或者“手动分配IP地址”。 选择“手动分配IP地址”后，可查看已使用的IP地址。

参数	示例	说明
安全组	**Sys-default**	选择当前区域下安全组，系统默认安全组**Sys-default**。 若无合适安全组可选择，可单击“管理安全组”创建或配置新的安全组。 **说明** • 一个安全组为同一个VPC网络内具有相同安全保护需求，并相互信任的CBH与资源提供访问策略。当云堡垒机加入安全组后，即受到该安全组中访问规则的保护。详细介绍请参见**安全组简介**。 • 云堡垒机可与资源主机ECS等共用安全组，各自调用安全组规则互不影响。 • 如需修改安全组，请参见**更改安全组**章节。 • 在创建HA实例前，需要安全组在入方向中放通22、31036、31679、31873这四个端口。 • 堡垒机创建时会自动开放80、8080、443、2222共四个端口，创建完成后若不需要使用请第一时间关闭。 • 堡垒机主备实例跨版本升级还会自动开放22、31036、31679、31873共四个端口，升级完成后保持31679开放即可，其余端口若不需要使用请第一时间关闭。 更多关于安全组的信息，请参见**配置云堡垒机安全组**。
弹性IP	**100.x.x.x**	（可选参数）选择当前区域下EIP。 若当前区域无可选EIP，可单击“购买弹性IP”创建弹性IP。
企业项目	**default**	选择此次购买的堡垒机所属的企业项目。 默认选择为“default”。
登录密码	**Cbh@shanghai.10**	自定义**admin**用户密码信息。 **说明** • 密码设置要求 – 长度范围：8~32个字符，不能低于8个字符，且不能超过32 个字符。 – 规则要求：可设置英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（!@$%^-_=+[{}]:,./?~#*），且需同时至少包含其中三种。 – 不能包含用户名或倒序的用户名。 – 不能包含超过2个连续的相同字符。 • 需设置和确认输入两次密码信息，两次输入信息需一致才能成功设置密码。 • 云堡垒机系统无法获取系统管理员**admin**用户密码，请务必保存好登录账号信息。 • 系统管理员**admin**在首次登录云堡垒机系统时，请按照系统提示修改密码和配置手机号码，否则无法进入云堡垒机系统。 • 完成实例购买后，若忘记**admin**用户密码，可参考**重置密码**解决。
购买时长	**1个月**	选择实例使用时长。 可按月或按年购买云堡垒机。

步骤5 配置完成后，查看“当前配置”确认信息，单击“立即购买”。

说明

当收到网络限制提示时，请先“一键放通”网络限制，确保购买实例后授权下发成功。

您可以在安全组和防火墙ACL中查看相应规则。

- 云堡垒机所在安全组允许访问出方向9443端口；
- 云堡垒机所在子网未关联防火墙ACL，或关联的防火墙ACL为“开启”状态且允许访问出方向9443端口。

步骤6 进入“订单详情”页面，确认订单无误并阅读《隐私政策声明》后，勾选“我已阅读并同意《隐私政策声明》”，单击“提交订单”。

步骤7 在支付页面完成付款，返回云堡垒机控制台页面，在“云堡垒机实例”列表下查看新购买的实例。

购买实例成功后，后台自动创建CBH系统，大约需要10分钟。

说明

后台创建CBH系统完成前，即实例的“状态”未变为“运行”前，请勿解绑EIP，否则可能导致CBH系统创建失败。

----结束

步骤二：登录堡垒机

堡垒机的纳管、运维、审计等操作均需登录至实例进行操作。

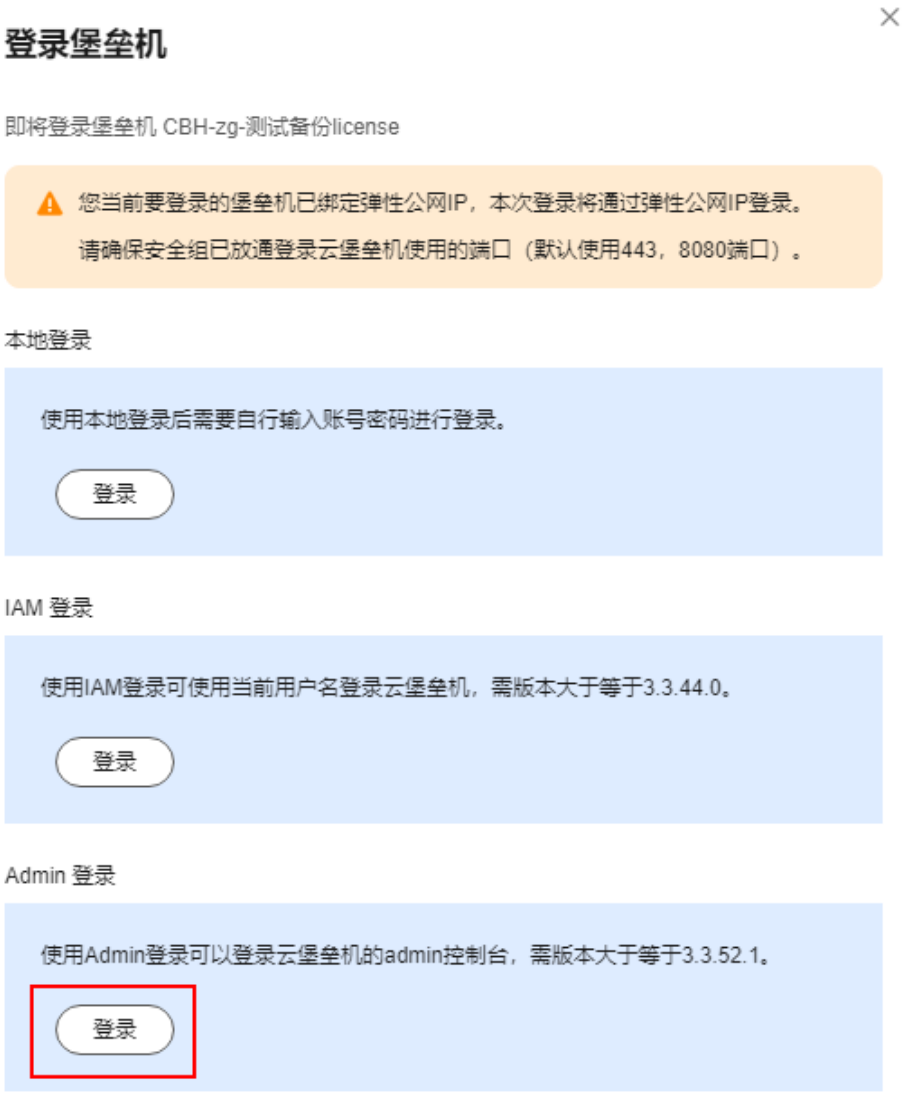
步骤1 返回云堡垒机实例列表页面，查看购买的云堡垒机“运行状态”为“运行”。

步骤2 单击“操作”列“远程登录”，在弹窗中单击“Admin登录”的“登录”按钮，将自动登录堡垒机实例。

说明

首次登录需要修改admin原始密码后才能正常进入堡垒机实例。

图 1-2 登录堡垒机



----结束

步骤三：添加资源

将资源添加至堡垒机后，才可通过堡垒机对资源进行审计或运维。

步骤1 在堡垒机实例页面选择“资源 > 主机管理”，进入主机管理列表页面。

如果需要添加应用资源，选择“资源 > 应用发布”，详情请参见**通过堡垒机纳管应用服务器**。

步骤2 单击“新建”，弹出新建主机编辑窗口，配置主机资源的网络参数和基础信息。

图 1-3 新建单个主机资源

表 1-3 主机资源网络参数说明

参数	示例	说明
主机名称	**host-shanghai-01**	自定义的主机资源名称，系统内“主机名称”不能重复。
协议类型	**SSH**	根据需要添加主机的协议类型选择。
主机地址	**100.x.x.x**	输入主机与堡垒机网络通畅的IP地址。

参数	示例	说明
端口	**22**	输入能正常访问主机的端口号。
系统类型	**Linux**	（可选）选择主机的操作系统类型或者设备系统类型。 • 默认为空，需要根据添加的资源系统类型选择对应的系统类型。 • 支持14种系统类型，包括Linux、Windows、Cisco、Huawei、H3C、DPtech、Ruijie、Sugon、Digital China sm-s-g 10-600、Digital China sm-d-d 10-600、ZTE、ZTE5950-52tm、Surfilter、ChangAn。 • 同时支持系统管理员**admin**自定义系统类型。
编码	**UTF-8**	“协议类型”选择“SSH”、“TELNET”协议类型主机时，可选择运维界面中文编码。 可选择UTF-8、Big5、GB18030。
终端类型	**Linux**	“协议类型”选择“SSH”、“TELNET”协议类型主机可选择运维终端类型。 可选择Linux、Xterm。
更多选项	**默认即可**	（可选）选择配置文件管理、X11转发、上行剪切板、下行剪切板、键盘审计。 • 文件管理：仅SSH、RDP、VNC协议类型主机可配置。 • 剪切板：仅SSH、RDP、TELNET协议类型主机可配置。 • X11转发：仅SSH协议类型主机可配置。 • 键盘审计：仅RDP、VNC、协议类型主机可配置。
所属部门	**总部**	选择主机所属部门。

步骤3 单击“下一步”，为纳管的主机资源添加账户，选择“以后添加”。

图 1-4 添加资源账户

步骤4 单击“确定”，且资源账户验证通过后，返回主机列表查看添加的主机资源。

----结束

步骤四：添加访问控制策略

资源添加后，需要为资源绑定账户或访问IP，以确保资源的访问安全性。

步骤1 在堡垒机实例选择“策略 > 访问控制策略”，进入策略列表页面。

步骤2 单击“新建”，弹出策略基本属性配置窗口，配置策略基本信息。

图 1-5 添加访问控制策略

步骤3 单击“下一步”，选择当前策略关联的用户admin。

图 1-6 选择关联用户

步骤4 单击“下一步”，选择当前策略关联的资源账户。

说明

资源账户“Empty”为添加资源时为资源自动创建的账户，用来登录资源使用。

图 1-7 关联资源账户

步骤5 单击“确定”，可在策略列表查看新建的策略。

说明

完成策略配置后，可在“运维 > 主机运维”列表页面选择目标主机使用“Empty”账户执行登录操作，登录后可执行运维操作，返回堡垒机实例选择“审计 > 系统日志”可查看登录日志和操作日志。

----结束

后续操作

- 如果有管理角色区分需求，可通过admin登录堡垒机在堡垒机实例添加不同的角色进行权限的细分管理，详情请参见**用户管理**。
- 如果对登录、账户、会话、网关、路由器、端口、认证、告警有自定义设置需求，可在“系统 > 系统配置”中进行配置，详情请参见**系统配置**。

2 入门实践

当您配置完云堡垒机（CBH）后，可以根据自身业务的业务场景使用CBH提供的一系列常用实践。

表 2-1 常用最佳实践

实践		描述
变更规格	变更堡垒机规格	当使用的云堡垒机规格不能满足实际需求时，您可以选择对云堡垒机的规格进行变更规格。
系统策略	数据库控制策略：高危命令二次审批	云堡垒机支持通过执行命令运维数据库，包括数据删除、修改、查看等运维操作。为确保数据库敏感信息的安全，避免关键信息的丢失和泄露，本文针对运维用户访问和运维数据库关键信息，详细介绍了如何设置数据库高危操作的复核审批，以及如何实现关键信息的重点监控。
等保合规	云堡垒机等保合规相关项	为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。
系统运维	跨云跨VPC线上线下统一运维	针对您的服务器资源分布在跨VPC、线下IDC机房、非华为云等跨网络域的场景，华为云堡垒机提供了通过网络代理服务器进行运维的方案，便于您在没有搭建网络专线的情况下，纳管各网络域的各类服务器资源，从而通过华为云堡垒机统一管理、运维您的各类工作负载。

实践		描述
运维审计	使用堡垒机对安全事故进行事后追溯	华为云堡垒机可以管控所有的操作，并对所有的操作都进行详细记录。针对会话的审计日志，支持在线查看、在线播放和下载后离线播放。目前支持字符协议（SSH、TELNET）、图形协议（RDP、VNC）、文件传输协议（FTP、SFTP、SCP）、数据库协议（DB2、MySQL、Oracle、SQL Server）和应用发布的操作审计。其中，字符协议和数据库协议能够进行操作指令解析，还原操作指令；文件传输能够记录传输的文件名称和目标路径。