云堡垒机(CBH)

产品介绍

文档版本 01

发布日期 2022-12-01

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 云堡垒机

云堡垒机（Cloud Bastion Host，CBH）是华为云的一款4A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。

云堡垒机提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

服务特点

- 一个实例对应一个独立运行的系统，通过配置实例部署系统后台运行基本环境。系统环境独立管理，保障系统运行安全。
- 一个单点登录系统，提供统一的单点登录入口，轻松地集中管理大规模云上资源，避免资源账户泄露危险，保障资源信息安全。
- 符合“网络安全法”等法律法规，满足合规性规范审查要求。
  - 满足《萨班斯法案》和《等级保护》系列文件中的技术审计要求；
  - 满足金融监管部门的技术审计要求；
  - 满足各类法令法规（如SOX、PCI、企业内控管理、等级保护、ISO/IEC27001等）对运维审计的要求。

2 功能特性

云堡垒机不仅拥有传统4A安全管控的基本功能特性，包括身份认证、账户管理、权限控制、操作审计四大功能。还拥有高效运维、工单申请等特色功能。

身份认证

采用多因子认证和远程认证技术，加强用户身份认证管理。

- 引用多因子认证技术，包括手机短信、手机令牌、USBKey、动态令牌等方式，安全认证登录用户身份，降低用户账号密码风险。
- 对接第三方认证服务或平台，包括AD域、RADIUS、LDAP、Azure AD远程认证，支持远程认证用户身份，防止身份泄露。并支持一键同步AD域服务器用户，复用原有用户部署结构。

账户管理

集中管理系统用户和资源账号信息，对账号全生命周期建立可视、可控、可管运维体系。

表 2-1 账号管理功能说明

功能特性	功能说明
用户账号管理	系统用户账号全生命周期管理，用户使用唯一账号登录系统，解决共享账号、临时账号、滥用权限等问题。 • 批量导入 通过同步第三方服务器用户，以及批量导入用户，支持一键同步并导入已有用户信息，无需重复创建用户。 • 用户组 用户账号按属性分组管理，可实现对同类型用户按用户组赋予权限。 • 批量管理 支持批量管理用户账号，包括删除、启用、禁用、重置密码、修改用户基本配置等。

功能特性	功能说明
资源账户管理	集中资源账户管理，资源账户全生命周期管理，实现单点登录资源，管理或运维无缝切换。 ● 资源类型 纳管资源类型丰富，包括Windows、Linux等主机资源，MySQL、Oracle等数据库资源，以及Windows应用程序资源。 – 支持C/S架构运维接入，包括SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、SQL Server、Oracle、SCP、Rlogin协议类型主机资源。 – 支持B/S、C/S架构应用系统资源接入，可直接配置12+种Edge、Chrome、Oracle Tool等浏览器或客户端Windows服务器应用资源。 ● 资源管理 – 批量导入 通过自动发现、同步云上资源，以及批量导入资源，支持一键同步并导入云上ECS、RDS等服务器上资源。 – 账户组管理 资源账户按属性分组管理，可实现对同类型资源账户按账户组给用户赋权 – 密码自动代填 采用AES256加密方式存储资源账户，通过密码自动代填技术加密共享账户，避免账户泄露风险。 – 账户自动改密 通过设置改密策略，可定时定期修改账户密码，确保资源的账户安全。 – 账户自动同步 通过设置账户同步策略，可定时定期核查和同步主机资源账户，包括拉取主机账户统计异常系统资源账户，以及推送系统新建、删除、修改的资源账户到主机，确保资源账户健康生存周期。 – 批量管理 支持批量管理资源信息和资源账户，包括删除资源、添加资源标签、修改资源信息、验证资源账户、删除资源账户等。

权限控制

集中管控用户访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置，保障了系统管理安全和资源运维安全。

表 2-2 权限控制功能说明

功能特性	功能说明
系统访问权限	从单个用户账号属性出发，控制用户登录和访问系统权限。 ● 用户角色 通过为每个用户账号分配不同的角色，赋予用户访问系统不同模块的权限，对系统用户身份进行分权。 系统支持自定义角色，自定义角色中可以自选添加系统模块，实现角色多样化模式。 ● 组织部门 通过为每个用户划分部门，采用部门组织树形结构，不限制部门层级，可将用户按部门分层级管理。 ● 登录限制 通过设置用户登录配置，从登录有效期、登录时间、多因子认证、登录IP限制、登录MAC限制等维度，赋予用户登录系统的权限。
资源访问权限	按照用户、用户组与资源账户、账户组之间的关联关系，建立用户对资源的控制权限。 ● 访问控制 通过设置访问控制权限，从访问有效期、登录时间、IP限制、上传/下载、文件传输、剪切板、显示水印等维度，赋予用户访问资源的权限。 ● 双人授权 通过设置双人或多人授权审核，需要授权人实时授权才能访问资源，保障敏感核心资源安全。 ● 命令拦截 通过设置命令控制策略或数据库控制策略，对服务器或数据库中敏感、高危操作，强制阻断、告警及二次复核，加强对关键操作的管控。 ● 批量授权 通过用户组和账户组形式，支持同时授权多个用户以多个资源的控制权限。

操作审计

基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。

表 2-3 操作审计功能说明

功能特性	功能详情
系统行为审计	系统操作行为全纪录，针对操作失误、恶意操作、越权操作等行为告警通知。 ● 系统登录日志 详细记录登录系统的方式、登录用户、用户来源IP、登录时间等信息。支持一键导出全部系统登录日志。 ● 系统操作日志 系统操作行为全程记录，覆盖所有系统操作事件。支持一键导出全部系统操作日志。 ● 系统报表 集中可视化呈现用户在系统的操作统计信息，包括用户启用状态、用户与资源创建、用户登录方式、异常登录、会话控制等信息。 支持一键导出系统报表，并可定周期以邮件方式自动推送系统报表。 ● 告警通知 通过配置系统告警，针对系统操作和系统环境制定不同告警方式和告警级别，以邮件方式和系统消息方式推送告警通知，以便及时发现系统异常和用户异常操作。

功能特性	功能详情
资源运维审计	全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。 ● 运维审计技术 – Linux命令审计 基于字符协议（SSH、TELNET）的命令操作审计，记录命令运维全程，支持解析字符操作命令，还原操作指令，根据输入、输出结果关键字搜索快速定位回放。 – Windows操作审计 基于图形协议（RDP、VNC）终端和应用发布的行为操作审计，远程桌面的操作全纪录，包括键盘操作、功能键操作、鼠标操作、窗口指令、窗口切换、剪切板拷贝等。 – 数据库命令审计 基于数据库协议（DB2、MySQL、Oracle、SQL Server）的命令操作审计，记录从SSO单点登录数据库到数据库命令操作全程，支持解析数据库操作指令，100%还原操作指令。 – 文件传输审计 基于远程桌面的文件传输操作审计，以及基于文件传输协议（FTP、SFTP、SCP）的传输操作审计，对Web浏览器或客户端文件传输全程审计，记录传输的文件名称和目标路径。 ● 运维审计形式 – 实时监控 实时查看正在进行的运维会话，支持监控和中断实时会话。 – 历史日志 运维操作全程记录，详细记录历史运维会话信息，支持一键导出历史会话日志。 – 会话视频 支持对Linux命令审计、Windows操作审计全程录像记录，回放录像视频。 支持生成视频文件，一键下载会话视频。 – 运维报表 集中可视化呈现运维统计信息，包括运维时间分布、资源访问次数、会话时长、双人授权、命令拦截、字符数命令、传输文件数等信息。 支持一键导出运维报表，并可定周期以邮件方式自动推送系统报表。 – 日志备份 通过配置日志备份，可将历史会话日志远程备份至Syslog服务器、FTP/SFTP服务器、OBS桶，实现系统日志容灾备份。

高效运维

通过多种架构运维、多种运维资源、多种运维工具、多种运维形式的接入，全面提升运维效率。

表 2-4 高效运维功能说明

功能特性	功能说明
Web浏览器运维	HTML5远程登录资源，无需安装客户端，一键登录运维资源，实现操作实时监控、文件上传下载等运维管理。 ● 一站式登录运维 在Windows、Linux、Android、iOS等操作系统上，支持任意主流浏览器无插件化运维，包括Edge、Chrome、Firefox等主流浏览器，让运维人员脱离运维工具和操作系统束缚，随时随地远程运维。 ● 批量登录 支持一键登录多个授权资源，多个资源可同时在一个浏览器页签运维。 ● 协同会话 支持多人参与“协同分享”，邀请其他运维人员或专家进行协同运维，对同一会话进行协同操作或问题定位，提高多人运维效率。 ● 文件传输 基于WSS的文件管理技术，支持文件上传/下载，以及文件在线管理，实现多主机文件共享功能 。 ● 命令群发 针对多个Linux资源，开启群发键。在一个会话窗口执行命令后，其他会话窗口将同步执行相同操作。
第三方客户端运维	在不改变用户使用原来客户端习惯的前提下，支持一键接入多种运维工具，提升运维效率。 ● 多种运维工具 支持接入SecureCRT、Xshell、Xftp、WinSCP、Navicat 、Toad for Oracle等工具。 ● SSH客户端运维 针对字符协议类主机资源，可通过运维客户端登录资源，实现运维平台多种选择。 ● 数据库客户端运维 针对数据库主机资源，通过配置SSO单点登录工具，调用数据库客户端，实现一键登录目标数据库资源，数据库运维操作。 ● 文件传输客户端运维 针对文件传输协议类主机资源，通过调用FTP/SFTP客户端登录资源，实现客户端运维。
自动化运维	线上多步骤复杂操作自动化执行，告别枯燥的重复工作，提高工作效率。 ● 脚本管理 线下脚本上线管理，支持Shell和Python类型脚本的管理。 ● 运维任务 通过配置命令执行、脚本执行、文件传输的运维任务，可定期、批量、自动执行预置的运维任务。

工单申请

系统运维用户在运维过程中，遇到需运维资源而无权限情况，可提交系统工单申请资源控制权限，寻求管理人员授权审批。

- 系统运维人员
  - 通过手动或自动触发工单系统，提交访问授权工单、命令授权工单、数据库授权工单申请权限。
  - 支持提交工单、查询工单、撤销工单、删除工单等功能。
- 系统管理人员
  - 通过自定义审批流程，支持多级审批。
  - 支持批准单个工单、批量批准工单、驳回工单、撤销工单、查询工单、删除工单等功能。

3 产品优势

HTML5 一站式管理

无需安装特定客户端，无需安装任何插件，任意终端的主流浏览器，包括移动端APP浏览器登录，用户随时随地打开即可进行运维。

系统HTML5管理界面简洁易用，集中管理用户、资源和权限，支持批量创建用户、批量导入资源、批量授权运维、批量登录资源等高效运维管理方式。

操作指令准确拦截

针对资源敏感操作进行二次复核，系统预置标准Linux字符命令库或自定义命令，对运维操作指令和脚本的准确拦截，并可通过异步“动态授权”，实现对敏感操作的动态管控，防止误操作或恶意操作的发生。

核心资源二次授权

借鉴银行金库授权机制，针对重要资源的运维权限设置多人授权，若需登录此类资源，需多位授权候选人进行“二次授权”，加强对核心资源数据的保护，提升数据安全防护能力和管理能力，保障核心资产数据的安全。

应用发布扩展

针对数据库类、Web应用类、客户端程序类等不同应用资源，提供统一访问入口，并可提高对应用操作的图形化审计。

数据库运维审计

针对DB2、MySQL、SQL Server和Oracle等云数据库，支持统一资源运维管理，以及SSO单点登录工具一键登录数据库，提供对数据库操作的全程记录，实现对云数据库的操作指令进行解析，100%还原操作指令。

自动化运维

自动化运维是将系统运维管理中复杂的、重复的、数量基数大的操作，通过统一的策略、任务将复杂运维精准化和效率化，帮助运维人员从重复的体力劳动中解放出来，提高运维效率。

4 应用场景

任何企业都需要安全运维管理和审计，故任何企业都需要云堡垒机。云堡垒机能适用于各种企业运维场景，特别针对企业员工数量复杂、企业资产数量繁杂、人员运维权限交叉、企业运维方式多样等场景。

严要求的审计合规场景

例如保险和金融行业，具有大量个人信息数据和金融资金操作行为，以及大量第三方机构代为运作，可能存在巨大违规操作、滥用职权等非法运作风险。

通过在云上部署云堡垒机系统，单点登录入口，集中管理账户和资源，部门权限隔离，核心资产多人审核授权，敏感操作二次复核授权，健全的运维审计机制，能够为高风险行业提供严要求审计功能，满足行业监管要求。

高效稳定的运维场景

例如极速发展的互联网企业，大量经营数据等敏感信息，暴露在公网，且由于服务高度公开，存在高度数据泄露风险。

云堡垒机在远程运维过程中，隐藏资产真实地址，解决远程运维资产信息暴露问题。同时提供全面的运维日志，为审计运维和代运维人员的操作行为，提供有效监控，减少网上安全事故，助力企业长久稳定发展。

大量资产和人员管理场景

随着民生政务和传统企业集团的上云管理，云上人员账户数量不断增加，以及云上服务器、网络设备等资产数量也成倍增涨。同时很多企业为解决人力不足的问题选择把系统运维转交给系统供应商或第三方代维商进行，由于涉及提供商、代维商过多，人员复杂流动性又大，对操作行为缺少监控带来的风险日益凸显。

云堡垒机针对大量用户和大量资产，可海量容纳庞大人员和资源数据，运维人员单点登录，解决运维人员维护多台资产效率低，易出错的问题。同时通过制定细粒度权限控制，资源操作全程记录，可审计全量用户操作行为，并对事故问题进行有效追溯，确保有效定责。此外，系统桌面实时呈现运维全景，并可接收异常行为告警通知，确保人员无法越权操作。

5 服务版本差异

目前云堡垒机提供**标准版**和**专业版**两个功能版本，标准版版本配备10、20、50、100、200、500、1000、2000、5000、10000资产规格，专业版配备10、20、50、100、200、500、1000、2000、5000、10000资产规格。

更多版本规格说明，请参见**云堡垒机规格版本**。

规格差异

云堡垒机支持10、20、50、100、200、500、1000、2000、5000、10000资产规格配置，不同规格云堡垒机配置差异，请参见**表1 不同规格配置说明**。

表 5-1 不同规格配置说明

资产数	最大并发数	CPU	内存	系统盘	数据盘
10	10	4核	8GB	100GB	200GB
20	20	4核	8GB	100GB	200GB
50	50	4核	8GB	100GB	500GB
100	100	4核	8GB	100GB	1000GB
200	200	4核	8GB	100GB	1000GB
500	500	8核	16GB	100GB	2000GB
1000	1000	8核	16GB	100GB	2000GB
2000	1500	8核	16GB	100GB	2000GB
5000	2000	16核	32GB	100GB	3000GB
10000	2000	16核	32GB	100GB	4000GB

须知

表 不同规格配置说明中的“并发数”是基于字符协议客户端运维（如SSH客户端、MySQL客户端）的并发数，基于图形协议运维（如H5 Web运维、RDP客户端运维）的并发数只有该值的1/3。

版本差异

标准版和**专业版**的基础功能均支持身份认证、权限控制、账户管理、操作审计，主要功能差异为自动化运维、数据库运维审计两个增强功能。

详细版本功能差异，请参见**表2 不同版本功能差异说明**。

表 5-2 不同版本功能说明

功能项	功能说明	标准版	专业版
身份认证	用户账号双因子认证 支持手机令牌、手机短信、USBKey、动态令牌等多因子认证形式。	√	√
	用户账号远程认证 支持AD域、RADIUS、LDAP、Azure AD远程认证。	√	√
权限控制	系统访问权限 通过划分组织部分结构、分配用户角色、设置用户登录限制，控制用户登录和访问系统权限。	√	√
	资源访问权限 按照用户、用户组、资源账户、账户组，建立用户对资源的访问控制授权，通过配置访问控制策略、双人授权、命令控制策略，实现对资源不同维度的控制。	√	√
	双人授权 通过配置“双人授权”实现双人或多人权限审核，保障核心资源安全。	√	√
	字符命令拦截 通过配置命令控制策略，对字符协议资源关键操作，进行动态授权。	√	√
	数据库命令拦截 通过配置数据库控制策略，对数据库资源敏感、危险等操作，进行精确限制、二次复核。 **说明** 数据库命令拦截功能不区分云数据库还是自建的数据库。	×	√
账户管理	用户账号全生命周期管理 • 用户账号单个创建、批量导入、批量管理，以及划分用户组管理。	√	√

功能项	功能说明	标准版	专业版
	资源账户全生命周期管理 ● 资源和资源账户的单个添加、批量导入、批量管理，以及资源账户的划分账户组管理。	√	√
	纳管主机资源 ● 支持纳管SSH、RDP、VNC、TELNET、FTP、SFTP、Rlogin协议类型的Linux和Windows资源。	√	√
	纳管应用资源 ● 支持通过Windows应用服务器，纳管Chrome、Edge、Firefox、Oracle Tool 、MySQL等浏览器或客户端应用资源。	√	√
	纳管数据库资源 ● 支持纳管DB2、MySQL、SQL Server和Oracle引擎类型数据库。	×	√
	资源账户自动改密 ● 通过配置改密策略，定期修改资源账户密码，管控资源账户及登录密码。	√	√
	资源账户自动同步 ● 通过配置账户同步策略，及时发现僵尸账户或未被管控账户。	×	√
操作审计	系统登录和操作全程记录 ● 支持导出系统日志、生成系统报表，以及配置告警通知。	√	√
	资源运维操作全程审计 ● 支持多种审计技术和审计形式，会话实时监控，历史会话可生成视频、导出文本报表的双重审计，并支持日志远程备份。	√	√
	数据库行为审计 ● 基于操作命令审计数据库运维全程。	×	√
高效运维	Web浏览器一站式运维 ● 远程登录资源，无需安装客户端，一键登录运维资源，并集成批量登录、协同会话、文件传输、命令群发等功能。	√	√
	第三方客户端运维 ● 一键接入多种运维工具，支持多种运维形式，包括SSH客户端运维、FTP/SFTP客户端运维等。	√	√
	数据库运维 ● 通过SSO单点登录工具调用客户端，一键登录目标数据库。	×	√

功能项	功能说明	标准版	专业版
	自动化运维 ● 在线管理脚本，以及定时执行预置运维任务。	×	√
工单申请	访问授权工单、命令授权工单申请 ● 系统用户为获取资源控制权限，通过手动或自动方式触发系统工单，提交工单给系统管理人员审批，获取权限的全程。	√	√
	数据库授权工单申请 ● 系统用户可触发数据库敏感操作，自动生成授权工单，系统用户需提交工单申请，由管理人员审批通过才能获取继续操作权限。	×	√

6 基本概念

云堡垒机实例

一个云堡垒机实例对应一个独立运行的云堡垒机系统，用户登录云堡垒机控制台管理实例。只有创建了云堡垒机实例后，才能登录云堡垒机系统，实现安全运维管理与审计。

单点登录

单点登录（Single Sign On，SSO）是指在多个独立应用系统环境下，各个应用系统相互信任，在一个应用系统中将用户认证信息映射到其他系统中，多个系统共享用户认证数据。简言之，即用户通过登录一个应用系统，就可以访问其他所有相互信任的应用系统，实现用户单点多系统登录。

资产数

资产数是指云堡垒机管理的云服务器上运行的资源数，同一台云服务器上对应有多个需要运维的协议、应用等资源。

例如，目前有一台云服务器，在云堡垒机中添加这台云服务器的资源，分别添加了2个RDP、1个TELNET和1个MySQL协议的主机资源，以及1个Chrome浏览器的应用资源，则当前管理的资产数即为5，而不是1。

并发数

并发数是指云堡垒机上同一时刻连接的运维协议连接数。

例如，10个运维人员同时通过云堡垒机运维设备，假设平均每个人产生5条协议连接（例如通过SSH客户端、MySQL客户端进行远程连接），则并发数等于50。

7 计费说明

计费项

云堡垒机实例按选购的版本规格和购买时长计费。

表 7-1 计费项说明

计费项	计费说明
云堡垒机实例	按购买实例的版本规格、购买时长计费。
实例购买时长	提供包月和包年的购买模式。
弹性公网IP	如果您需要通过公网登录CBH，那么您需要为CBH实例绑定EIP，且绑定EIP可用。弹性公网IP按带宽或流量**单独计费**，详情请参见**EIP计费说明**。 **说明** 为确保云堡垒机系统的正常部署和使用，在付费购买云堡垒机实例后，以及云堡垒机实例使用期间，请保持绑定的EIP可用。

说明

为正常使用**应用发布**功能，在通过应用发布管理资源前，**需另行购买**Windows类型主机、镜像、企业授权码、客户端License等资源，该部分资源费用不计入CBH计费项。

计费模式

云堡垒机实例的计费模式为包月和包年，暂不支持按需计费。

购买1年，在总价基础上享受83折优惠，购买2年享受7折优惠，购买3年享受5折优惠。对于长期用户，推荐包年购买。

详情请参见**云堡垒机价格详情**。

变更配置

- 变更规格实例规格

  当您的业务需求增加，可在计费周期内“变更规格”规格。支持从**标准版**变更规格到**专业版**，或更高规格**标准版**。不支持降级到低规格的版本。

- 退订

  购买云堡垒机实例后，如需停止使用，请到费用中心执行**退订**操作。

续费

包年/包月购买的云堡垒机到期后，您可以在“云堡垒机实例”列表页面，单击操作列的“更多 > 续费”，跳转至续费管理页面完成续费，延长使用期。续费成功后，后台自动更新云堡垒机系统授权时长。

更多续费信息（例如导出续费清单、变更资费等），请参见**续费管理**。

到期与欠费

包年/包月资源开通成功后，如果没有按时续费，会根据“客户等级”和“订购方式”定义不同的保留期时长。保留期内资源处理说明，详见**保留期**。

当您的账户欠费后，可查看欠费详情，此时账号将进入欠费状态，需要在约定时间内支付欠款。为避免相关资源不被停止或者释放，请及时为账户充值，详细操作请参考**欠费还款**。

8 安全

8.1 责任共担

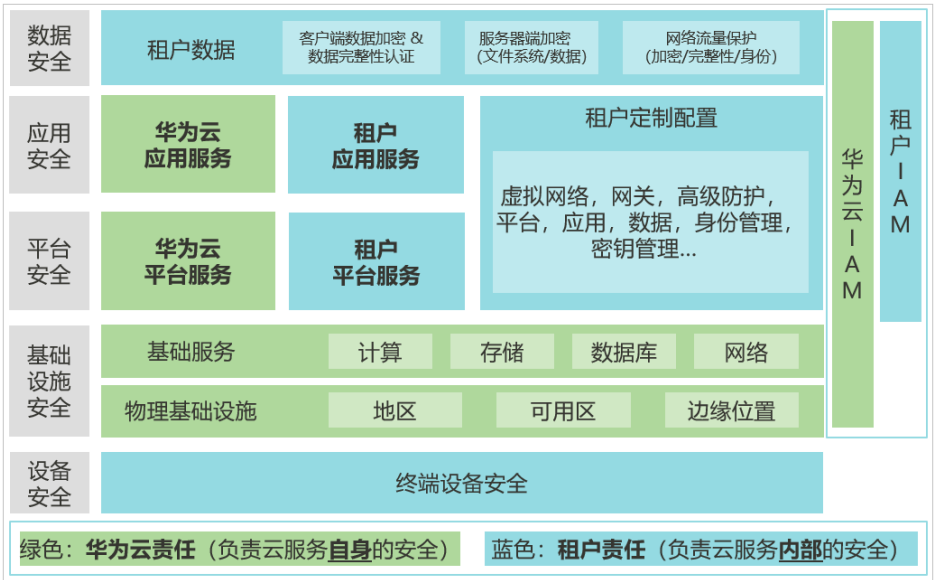
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图8-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



8.2 资产识别与管理

CBH服务已对接RMS服务，在华为云控制台右上角单击资源-我的资源便可查看用户所拥有的资源，例如弹性云服务器（ECS）、虚拟私有云（VPC）、对象存储服务（OBS）以及云堡垒机服务（CBH）等服务，通过RMS，可以查看各资源的详情，例如ECS的状态、规格等等。

云堡垒机支持添加SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、SQL Server、Oracle、SCP、Rlogin等协议类型的主机资源，包括Linux主机、Windows主机和数据库等，支持通过单个添加和批量导入的方式添加主机资源。此外，CBH支持纳管用户的应用服务器，支持添加Chrome、Edge、Firefox、SecBrowser、Oracle Tool 、MySQL、SQL Server Tool、dbisql、VNC Client、VSphere Client、Radmin等应用。

8.3 身份认证与访问控制

身份认证

用户访问CBH实例的方式有Web Console和SSH两种方式，其中，Web Console可以对堡垒机实例进行相关的资源配置和命令下发等完整功能，而SSH只能对堡垒机纳管的实例进行运维操作。

用户登录Web Console和SSH使用的账号和口令均为创建堡垒机时设置的账号和口令，此外，Web Console同样支持手机短信、手机令牌、USBKey、动态令牌的方式进行登录。

访问控制

CBH支持安全组、Web应用防火墙、ACL、VPC对堡垒机实例的访问进行权限控制。

表 8-1 CBH 支持的访问控制方式

访问控制方式		简要说明
权限控制	VPC	虚拟私有云（Virtual Private Cloud）是用户在华为云上申请的隔离的、私密的虚拟网络环境。用户可以基于VPC构建独立的云上网络空间，配合弹性公网IP、云连接、云专线等服务实现与Internet、云内私网、跨云私网互通，帮助打造可靠、稳定、高效的专属云上网络
	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云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。
	Web应用防火墙	华为云Web应用防火墙WAF对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，全面避免网站被黑客恶意攻击和入侵。

8.4 数据保护技术

云堡垒机实例不直接采集用户个人数据。实例创建成功后，登录云堡垒机系统需创建用户账号，创建登录系统用户账号涉及个人数据采集。

为了确保您的个人数据（例如云堡垒机系统登录名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，云堡垒机通过加密传输、加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围：

云堡垒机收集及产生的个人数据如下表所示：

服务	类型	收集方式	是否可修改	是否必须
云堡垒机实例	登录名	在创建用户账号时由系统管理员配置登录名	否	是 登录名是用户的身份标识信息
	密码	• 在管理员创建用户、重置用户密码时配置密码 • 在用户登录系统前重置密码、登录系统后修改密码时输入密码	是	是 用户登录云堡垒机系统时使用
	邮箱	• 在管理员创建用户时配置邮箱 • 在用户登录系统后修改邮箱时输入邮箱	是	是 接收系统邮件通知
	手机号	• 在管理员创建用户时配置手机号 • 在用户登录系统后修改手机时输入手机号	是	是 • 接收系统手机短息通知 • 在忘记密码时通过手机验证码重置密码

- **传输方式：**

CBH支持HTTP和HTTPS两种传输协议，为保证数据传输的安全性，推荐您使用更加安全的HTTPS协议。

- **存储方式：**

云堡垒机通过安全的加密算法对用户个人敏感数据加密后进行存储。

- 登录名：不属于敏感数据，明文存储
- 密码、邮箱、手机：加密存储
- **访问权限控制：**

云堡垒机系统用户个人数据通过加密存储，系统管理员及上级管理员需通过安全码才能查看用户的手机、邮箱。但用户密码对所有人（包括本人）都不明文可见。

- **二次认证：**

云堡垒机系统用户账号配置用户登录限制“**多因子认证**”后，用户在登录系统时开启登录验证功能，需要二次认证（二次认证方式支持“手机短信”、“手机令牌”、“USBKey”、“动态令牌”），有效保护用户敏感信息。

8.5 审计与日志

审计

云堡垒机系统用户个人数据的所有操作，包括增加、修改、查询和删除，云堡垒机系统都会记录审计日志，并可备份到远程服务器或本地电脑。拥有审计权限用户可以查看并管理下级管理部门用户账号的日志，系统管理员Admin拥有系统最高权限，可查看并管理登录系统全部用户账号操作记录。

基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警：

表 8-2 云堡垒机审计功能特性

功能特性	功能详情
系统行为审计	系统操作行为全纪录，针对操作失误、恶意操作、越权操作等行为告警通知。 ● 系统登录日志 详细记录登录系统的方式、登录用户、用户来源IP、登录时间等信息。支持一键导出全部系统登录日志。 ● 系统操作日志 系统操作行为全程记录，覆盖所有系统操作事件。支持一键导出全部系统操作日志。 ● 系统报表 集中可视化呈现用户在系统的操作统计信息，包括用户启用状态、用户与资源创建、用户登录方式、异常登录、会话控制等信息。 支持一键导出系统报表，并可定周期以邮件方式自动推送系统报表。 ● 告警通知 通过配置系统告警，针对系统操作和系统环境制定不同告警方式和告警级别，以邮件方式和系统消息方式推送告警通知，以便及时发现系统异常和用户异常操作。

功能特性	功能详情
资源运维审计	全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。 ● 运维审计技术 Linux命令审计 基于字符协议（SSH、TELNET）的命令操作审计，记录命令运维全程，支持解析字符操作命令，还原操作指令，根据输入、输出结果关键字搜索快速定位回放。 ● Windows操作审计 基于图形协议（RDP、VNC）终端和应用发布的行为操作审计，远程桌面的操作全纪录，包括键盘操作、功能键操作、鼠标操作、窗口指令、窗口切换、剪切板拷贝等。 ● 数据库命令审计 基于数据库协议（DB2、MySQL、Oracle、SQL Server）的命令操作审计，记录从SSO单点登录数据库到数据库命令操作全程，支持解析数据库操作指令，100%还原操作指令。 ● 文件传输审计 基于远程桌面的文件传输操作审计，以及基于文件传输协议（FTP、SFTP、SCP）的传输操作审计，对Web浏览器或客户端文件传输全程审计，记录传输的文件名称和目标路径。 ● 运维审计形式 实时监控 实时查看正在进行的运维会话，支持监控和中断实时会话。 ● 历史日志 运维操作全程记录，详细记录历史运维会话信息，支持一键导出历史会话日志。 ● 会话视频 支持对Linux命令审计、Windows操作审计全程录像记录，回放录像视频。 支持生成视频文件，一键下载会话视频。 ● 运维报表 集中可视化呈现运维统计信息，包括运维时间分布、资源访问次数、会话时长、双人授权、命令拦截、字符数命令、传输文件数等信息。 支持一键导出运维报表，并可定周期以邮件方式自动推送系统报表。 ● 日志备份 通过配置日志备份，可将历史会话日志远程备份至Syslog服务器、FTP/SFTP服务器、OBS桶，实现系统日志容灾备份。

日志

堡垒机本身支持管理改密日志、执行日志、查看系统日志和审计运维日志功能。

同时堡垒机实例内已对接云日志服务（Log Tank Service，简称LTS），可以向用户提供日志收集、分析、存储等服务。用户可以通过云日志服务快速高效地进行设备运维管理、用户业务趋势分析、安全监控审计等操作。

LTS的详细介绍和开通配置方法，请参见配置LTS日志外发功能。

日志记录

云堡垒机系统用户个人数据的所有操作，包括增加、修改、查询和删除，云堡垒机系统都会记录审计日志，并可备份到远程服务器或本地电脑。拥有审计权限用户可以查看并管理下级管理部门用户账号的日志，系统管理员Admin拥有系统最高权限，可查看并管理登录系统全部用户账号操作记录。

8.6 服务韧性

CBH通过多活无状态的跨AZ部署、AZ之间数据容灾等技术方案，保证业务进程故障时快速启动并修复，以保障服务的持久性和可靠性。

同时，基于华为云平台的防护能力，防御DoS攻击。

8.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 8-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 8-3 资源中心

9 使用限制

为提高云堡垒机安全管理系统的稳定性和安全性，在CBH实例和系统的使用上有固定一些限制。

网络访问限制

- 不支持跨区域（Region）直接使用。

  云堡垒机实例与系统资源（系统内管理的弹性云服务器、云数据库等）必须在同一区域内。

  虽跨区域跨VPC可通过**虚拟专用网（Virtual Private Network，VPN）**等构建跨区域网络，但受限于网络的不稳定性，不建议跨区域使用云堡垒机纳管资源。
- 不支持跨VPC直接使用。

  云堡垒机实例与系统资源必须在同一个VPC的子网内，才能直接连接访问。

  跨VPC情况下，可通过**对等连接**打通两个VPC之间网络。
- 云堡垒机实例与系统资源的安全组，必须允许相互访问。

  系统资源必须处于实例所属安全组允许访问的范围内，且资源所属安全组必须允许实例私有IP访问。

  如果实例与系统资源处于不同的安全组，系统默认不能访问。需要在实例的安全组添加“入”的访问规则。

  实例的安全组默认端口有443和2222，默认支持Web浏览器和SSH客户端访问。若需其他访问方式，需用户手动添加目标端口。

  具体端口限制详见**表9-1**。
- 只允许通过IP地址和端口访问CBH系统。

表 9-1 入/出方向规则配置参考

场景描述	方向	协议/应用	端口
通过Web浏览器登录云堡垒机（HTTP、HTTPS）	入方向	TCP	80、443、8080
通过MSTSC客户端登录云堡垒机	入方向	TCP	53389
通过SSH客户端登录云堡垒机	入方向	TCP	2222

场景描述	方向	协议/应用	端口
通过FTP客户端登录云堡垒机	入方向	TCP	20~21
通过云堡垒机的SSH协议远程访问Linux云服务器	出方向	TCP	22
通过云堡垒机的RDP协议远程访问Windows云服务器	出方向	TCP	3389
通过云堡垒机访问Oracle数据库	入方向	TCP	1521
通过云堡垒机访问Oracle数据库	出方向	TCP	1521
通过云堡垒机访问MySQL数据库	入方向	TCP	33306
通过云堡垒机访问MySQL数据库	出方向	TCP	3306
通过云堡垒机访问SQL Server数据库	入方向	TCP	1433
通过云堡垒机访问SQL Server数据库	出方向	TCP	1433
通过云堡垒机访问DB数据库	入方向	TCP	50000
通过云堡垒机访问DB数据库	出方向	TCP	50000
通过云堡垒机访问GaussDB数据库	入方向	TCP	18000
通过云堡垒机访问GaussDB数据库	出方向	TCP	18000
License注册许可服务器	出方向	TCP	9443
华为云服务	出方向	TCP	443
同一安全组内通过SSH客户端登录云堡垒机	出方向	TCP	2222
短信服务	出方向	TCP	10743、443
DNS域名解析	出方向	UDP	53

支持管理的资源

您购买的非华为云或者云下服务器，只要与华为云云堡垒机网络互通并且协议互相支持，就可以通过云堡垒机纳管相应服务器。

- **支持的主机类型**

  支持SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin协议类型的Windows或Linux主机。
- **支持的数据库类别**
  - 关系型数据库（Relational Database Service，RDS）。
  - 弹性云服务器（Elastic Cloud Server ，ECS）的自建数据库。
- **支持的数据库类型及版本**

表 9-2 支持的数据库引擎及版本

数据库引擎	引擎版本
MySQL	5.5，5.6，5.7，8.0
Microsoft SQL Server	2014、2016、2017、2019、2022
Oracle	10g、11g、12c、19c、21c
DB2	DB2 Express-C
PostgreSQL	11、12、13、14、15
GaussDB	2、3

- **支持应用管理的服务器类型及版本**

  仅支持对Windows服务器和Linux上的应用进行管理 ，且支持的服务器系统版本如表9-3。

  表 9-3 支持的应用服务器类型及版本

系统类型	系统版本
Windows	Windows Server 2008 R2及以上版本
Linux	CentOS7.9

  说明

  目前仅X86版本云堡垒机支持应用运维，ARM版本云堡垒机不支持应用运维。

支持使用的第三方客户端

云堡垒机需通过第三方客户端登录CBH系统，以及调用第三方客户端，实现安全运维管理。

表 9-4 登录 CBH 支持的客户端及版本

登录方式	支持使用的客户端	版本
Web浏览器登录	Edge	44及以上版本 **说明** Edge浏览器上传大文件限制：文件上传到主机，支持单个文件最大4G。
	Chrome	52.0及以上版本
	Safari	10及以上版本
	Firefox	50.0及以上版本

登录方式	支持使用的客户端	版本
SSH客户端登录	SecureCRT	8.0及以上版本
	Xshell	5及以上版本
	Mac Terminal	2.0及以上版本

表 9-5 运维过程支持调用的客户端

运维方式	资源协议类型/应用类型	支持调用的客户端
数据库运维（主机运维方式）	MySQL	Navicat 11、12、15、16 MySQL Administrator 1.2.17 MySQL CMD DBeaver22、23
	SQL Server	Navicat 11、12、15、16 SSMS 17
	Oracle	Toad for Oracle 11.0、12.1、12.8、13.2 Navicat 11、12、15、16 PL/SQL Developer 11.0.5.1790 DBeaver22、23
	DB2	DB2 CMD命令行 11.1.0
文件传输运维	SFTP	Xftp、WinSCP、FlashFXP
	FTP	Xftp、WinSCP、FlashFXP、FileZilla
应用发布运维	MySQL Tool	MySQL Administrator
	Oracle Tool	PL/SQL Developer
	SQL Server Tool	SSMS
	dbisql	dbisql
	Chrome	Chrome
	Edge	Edge
	Firefox	Firefox
	VNC Client	VNC Viewer
	SecBrowser	SecBrowser
	VSphere Client	VSphere Client
	Radmin	Radmin

其他约束与限制

- 云堡垒机能纳管资源的最大数量不能超过实例规格的总资产数。
- 云堡垒机能同时登录运维资源的最大数量不能超过实例规格的总并发数。

说明

资产数是云堡垒机管理的云服务器上运行的资源数，同一个云服务器上对应有多个需要运维的协议、应用等资源。

并发数是云堡垒机同一时刻连接运维协议的连接数。

详细说明请参见**基本概念**。

10 CBH 实例权限管理

如果您需要对华为云上购买的云堡垒机（Cloud Bastion Host，CBH）实例资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望员工拥有云堡垒机（Cloud Bastion Host，CBH）实例的使用权限，但是不希望员工拥有创建、变更规格、升级CBH实例等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CBH实例，但是不允许创建、变更规格、升级CBH实例的权限策略，控制员工对CBH实例资源的使用范围

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CBH的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

CBH 实例权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CBH实例部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CBH实例时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业

对权限最小化的安全管控要求。例如：针对CBH实例，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。CBH实例支持的授权项请参见**权限及授权项**。

如**表10-1**所示，包括了CBH实例的所有系统权限。

表 10-1 CBH 实例系统权限

系统角色/策略名称	描述	类别	依赖关系
CBH FullAccess	云堡垒机实例的所有权限（支付权限除外）。	系统策略	无
CBH ReadOnlyAccess	云堡垒机实例只读权限，拥有该权限的用户仅能查看云堡垒机服务，不具备服务配置和操作权限。	系统策略	无

说明

您在赋予账号企业项目级的CBH FullAccess权限时，还需要授予账号IAM项目级别的CBH ReadOnlyAccess权限，这样才可以在华为云Console控制台正常使用CBH服务的各项功能。

如**表10-2**列出了CBH实例常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 10-2 常用操作与系统权限的关系

操作	CBH FullAccess	CBH ReadOnlyAccess
创建云堡垒机	√	x
变更云堡垒机规格（变更规格）	√	x
查询云堡垒机列表	√	√
升级云堡垒机软件版本	√	x
查询ECS配额	√	x
绑定或解绑EIP	√	x
重启云堡垒机	√	x
启动云堡垒机	√	x
关闭云堡垒机	√	x
查看云堡垒机可用区	√	x
检测当前配置是否支持创建IPv6云堡垒机	√	x

操作	CBH FullAccess	CBH ReadOnlyAccess
检测云堡垒机与License中心之间网络是否连通	√	x
修改云堡垒机网络，确保与License中心网络连通	√	x

相关介绍

- IAM产品介绍
- 创建用户组、用户并授予CBH实例权限
- CBH实例自定义策略
- CBH实例权限及授权项

CBH FullAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
                "Effect": "Allow",
                "Action": [
                   "cbh:*:*",
                   "vpc:subnets:get",
                   "vpc:publicIps:list",
                   "vpc:vpcs:list",
                   "vpc:securityGroups:get",
                   "vpc:firewallGroups:get",
                   "vpc:firewallPolicies:get",
                   "vpc:firewallRules:get",
                   "vpc:ports:get",
                   "vpc:publicips:update",
                   "vpc:securityGroups:create",
                   "vpc:firewallRules:create",
                   "vpc:firewallPolicies:addRule"
                   "ecs:cloudServerFlavors:get",
                   "evs:types:get"
         ]
      }
   ]
}
```

CBH ReadOnlyAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
                "Effect": "Allow",
                "Action": [
                   "cbh:*:list*",
                   "vpc:publicIps:list",
                   "vpc:vpcs:list",
                   "vpc:securityGroups:get",
                   "vpc:subnets:get"
         ]
      }
```

```
  ]
}
```


11 基于 IAM 进行权限管理

如果您需要对华为云上购买的CBH资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用CBH服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有CBH的使用权限，但是不希望他们拥有删除CBH等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用CBH，但是不允许删除CBH的权限，控制他们对CBH资源的使用范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 11-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	• 系统角色 • 系统策略 • 自定义策略	为主体授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	• 系统策略 • 自定义身份策略	• 为主体授予身份策略 • 身份策略附加至主体	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快速地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色与策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在身份策略中通过条件键“g:RequestedRegion”的配置即可达到身份策略对于授权区域的控制。将身份策略附加主体或为主体授予该身份策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。

关于IAM的详细介绍，请参见**IAM产品介绍IAM产品简介IAM产品简介**。

身份策略权限管理

CBH服务支持身份策略授权。默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CBH部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问CBH时，需要先切换至授权区域。

如**表1**所示，包括了CBH的所有系统权限。角色与策略授权场景的系统策略与身份策略授权场景的并不互通。

表 11-2 CBH 系统权限

系统角色/策略名称	描述	类别	依赖关系
CBH FullAccess	云堡垒机实例的所有权限（支付权限除外）。	系统策略	无

系统角色/策略名称	描述	类别	依赖关系
CBH ReadOnlyAccess	云堡垒机实例只读权限，拥有该权限的用户仅能查看云堡垒机服务，不具备服务配置和操作权限。	系统策略	无
CBH ServiceLinkedAgencyPolicy	云堡垒机服务访问租户密钥管理服务、凭据管理服务需要的委托权限。	系统策略	无

表11-3列出了CBH常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 11-3 常用操作与系统权限的关系

操作	CBH FullAccess	CBH ReadOnlyAccess	CBH ServiceLinkedAgencyPolicy
创建云堡垒机	√	x	x
变更云堡垒机规格（变更规格）	√	x	x
查询云堡垒机列表	√	√	x
升级云堡垒机软件版本	√	x	x
查询ECS配额	√	x	x
绑定或解绑EIP	√	x	x
重启云堡垒机	√	x	x
启动云堡垒机	√	x	x
关闭云堡垒机	√	x	x
查看云堡垒机可用区	√	x	x
检测当前配置是否支持创建IPv6云堡垒机	√	x	x
检测云堡垒机与License中心之间网络是否连通	√	x	x
修改云堡垒机网络，确保与License中心网络连通	√	x	x
访问租户密钥管理服务、凭据管理服务需要的委托。	√	x	√

CBH 控制台功能依赖的角色或策略

表 11-4 表 1 CBH 控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
创建堡垒机	弹性云服务器 ECS 虚拟私有云 VPC	IAM用户设置了CBH FullAccess权限后，需要增加ECS CommonOperations和VPC FullAccess后才能在控制台创建云堡垒机。
绑定/解绑EIP	弹性公网IP EIP	IAM用户设置了CBH FullAccess权限后，需要增加VPC FullAccess后才能在控制台为堡垒机绑定/解绑EIP。
更新堡垒机安全组	虚拟私有云 VPC	IAM用户设置了CBH FullAccess权限后，需要增加VPC FullAccess后才能在控制台为堡垒机更新安全组。

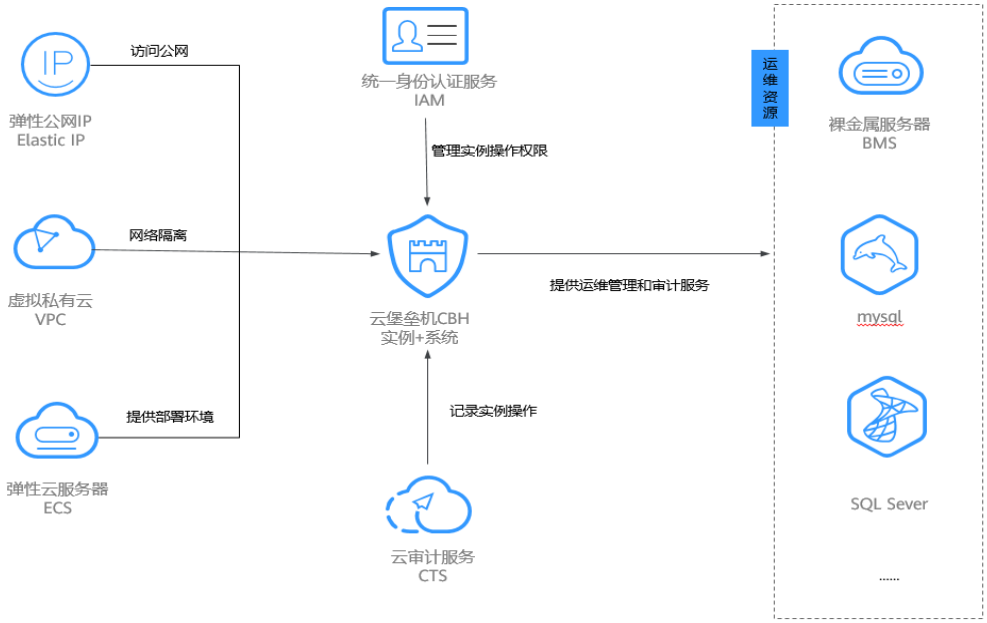
相关链接

- IAM产品介绍
- 通过IAM进行授权
- 身份策略授权参考

12 与其他云服务的关系

云堡垒机需要与其他云服务协同工作，与其他云服务的依赖关系如图12-1。

图 12-1 与其他云服务之间关系



与虚拟私有云的关系

虚拟私有云（Virtual Private Cloud，VPC）为CBH提供虚拟网络环境，用户通过配置安全组、子网、EIP等子服务，方便地管理、配置内部网络。以及通过自定义安全组内访问规则，加强安全保护。

与弹性云服务器的关系

弹性云服务器（Elastic Cloud Server，ECS）为CBH提供部署环境，同时CBH为ECS上资源提供安全管理服务。

- ECS为CBH系统后台提供部署环境，后台采用EulerOS操作系统。
- 用户通过CBH登录ECS上资源，为弹性云上面的服务器、数据库等资源，提供资产管理、登录身份管理、运维会话审计等功能，加强主机资源运维安全。

与弹性公网 IP 的关系

弹性公网IP（Elastic IP，EIP）为CBH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。一个弹性公网IP只能绑定一个云资源使用。EIP与CBH灵活绑定连接Internet，并支持灵活调整带宽，应对访问流量业务的变化。

与云数据库的关系

用户通过CBH登录**华为云关系型数据库**（Relational Database Service，RDS）（主要是MySQL、SQL Server两类数据库）数据库，为数据库资源提供资产管理、登录身份管理、运维会话审计等功能，加强数据库资源运维安全。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）为CBH实例提供云服务资源的操作记录，记录内容包括访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录CBH实例相关操作事件，方便用户日后的查询、审计和回溯，更多说明请参见**云审计支持的CBH操作**。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，IAM）为CBH实例提供用户身份鉴权、IAM用户权限设置等权限管理服务，更多详细说明请参见**CBH权限管理**。

13 个人数据保护机制

云堡垒机实例不直接采集用户个人数据。实例创建成功后，登录云堡垒机系统需创建用户账号，创建登录系统用户账号涉及个人数据采集。

为了确保您的个人数据（例如云堡垒机系统登录名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，云堡垒机通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

云堡垒机收集及产生的个人数据如表13-1所示：

表 13-1 个人数据范围列表

服务	类型	收集方式	是否可修改	是否必须
云堡垒机实例	登录名	在创建用户账号时由系统管理员配置登录名	否	是 登录名是用户的身份标识信息
	密码	• 在管理员创建用户、重置用户密码时配置密码 • 在用户登录系统前重置密码、登录系统后修改密码时输入密码	是	是 用户登录云堡垒机系统时使用
	邮箱	• 在管理员创建用户时配置邮箱 • 在用户登录系统后修改邮箱时输入邮箱	是	是 接收系统邮件通知
	手机	• 在管理员创建用户时配置手机号 • 在用户登录系统后修改手机时输入手机号	是	是 • 接收系统手机短息通知 • 在忘记密码时通过手机验证码重置密码

存储方式

云堡垒机通过加密算法对用户个人敏感数据加密后进行存储。

- 登录名：不属于敏感数据，明文存储
- 密码、邮箱、手机：加密存储

访问权限控制

云堡垒机系统用户个人数据通过加密存储，系统管理员及上级管理员需通过安全码才能查看用户的手机、邮箱。但用户密码对所有人（包括本人）都不明文可见。

二次认证

云堡垒机系统用户账号配置用户登录限制“多因子认证”后，用户在登录系统时开启登录验证功能，需要二次认证（二次认证方式支持“手机短信”、“手机令牌”、“USBKey”、“动态令牌”），有效保护用户敏感信息。

日志记录

云堡垒机系统用户个人数据的所有操作，包括增加、修改、查询和删除，云堡垒机系统都会记录审计日志，并可备份到远程服务器或本地电脑。拥有审计权限用户可以查看并管理下级管理部门用户账号的日志，系统管理员**admin**拥有系统最高权限，可查看并管理登录系统全部用户账号操作记录。

14 安全声明

在操作CBH前请仔细阅读，避免出现网络安全事件。

账户管理

云堡垒机系统的系统管理员默认账号为**admin**，登录密码为申请实例时自定义设置的密码。

在首次登录云堡垒机系统后，请按照系统提示修改密码，否则无法进入系统运行页面。

密码管理

为充分保证安全，建议您设置的各类密码满足以下要求：

- 在首次登录云堡垒机系统后，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。
- 密码必须满足密码安全策略：
  - 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，且需同时包含其中三种。
  - 不能设置为用户名或倒序的用户名。
- 建议定期修改密码，以提高登录账户的安全性。

特性声明

- 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。
- 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。
- 云堡垒机支持HTTPS访问协议，不支持HTTP访问协议。
- 请在法律法规允许的目的和范围内使用。

第三方软件

云堡垒机使用了以下第三方软件：

- 云堡垒机系统Web浏览器登录方式，建议使用浏览器和版本请参见**表14-1**。

  表 14-1 建议使用浏览器及版本

浏览器	版本	说明
Edge	44及以上版本	上传大文件限制：H5运维界面，文件上传到主机，支持单个文件最大4G。
Chrome	52.0及以上版本	-
Safari	10及以上版本	-
Firefox	50.0及以上版本	-

软件下载方式包含：

- 管理员用户账号成功登录云堡垒机系统后，单击桌面右上角“下载中心”， 单击相应软件下载。
- 运维用户账号成功登录云堡垒机系统后，单击桌面右上角“下载中心”， 单击相应软件下载。

A 修订记录

发布日期	修改说明
2022-12-01	第一次正式发布。