

云堡垒机

快速入门

文档版本 01
发布日期 2022-12-01



版权所有 © 华为技术有限公司 2022。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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

目录

1 使用前必读.....	1
2 步骤一：登录云堡垒机系统.....	4
3 步骤二：创建系统用户.....	10
4 步骤三：添加系统资源.....	12
5 步骤四：配置运维权限.....	16
6 步骤五：登录资源运维.....	18
7 步骤六：审计运维会话.....	19
A 修订记录.....	21

1 使用前必读

本文旨在帮助您了解云堡垒机（Cloud Bastion Host, CBH）入手使用的基本流程，帮助您更快上手操作。

- 通过Web浏览器、SSH客户端登录云堡垒机系统，依次创建用户、添加资源、配置权限策略，授予用户运维资源权限。
- 用户获取资源管理权限后，通过云堡垒机登录资源。
- 审计用户运维会话，以及审计用户登录系统和系统操作。

云堡垒机基础使用流程如[图1-1](#)所示。

图 1-1 使用流程

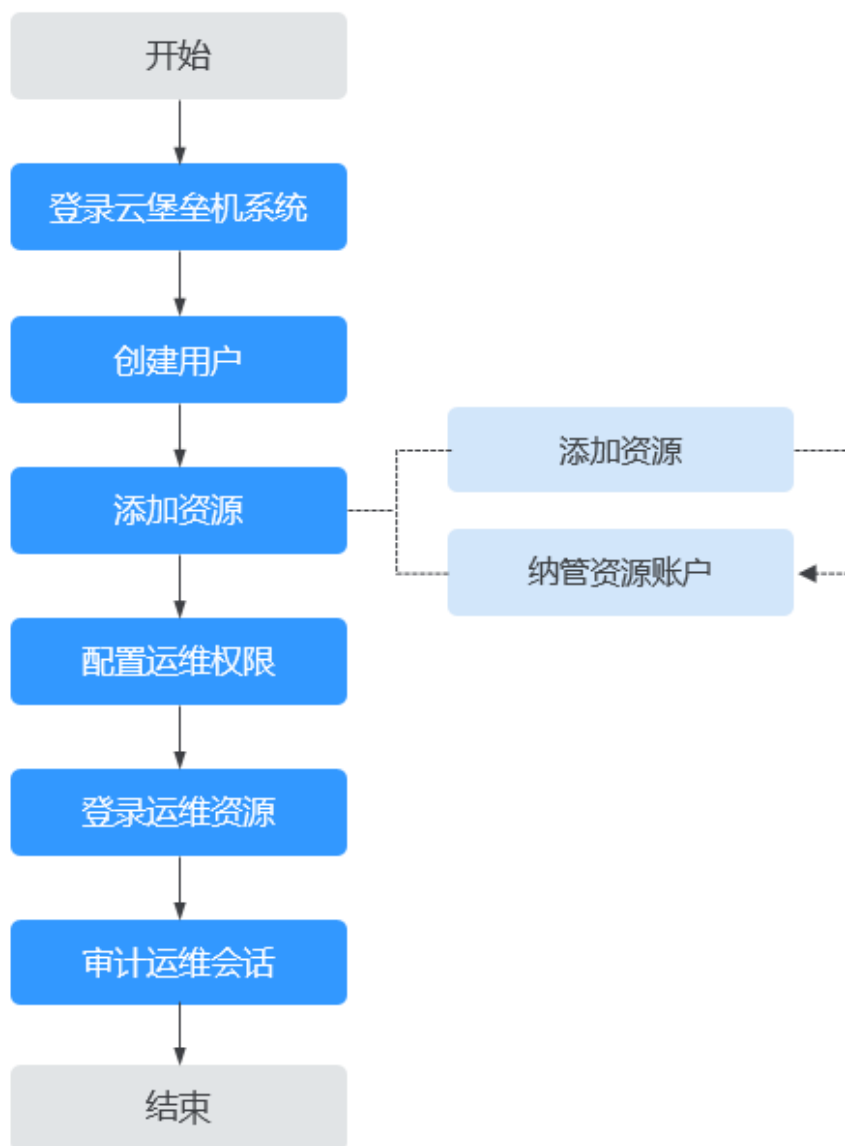


表 1-1 使用流程简介

操作步骤	说明
登录云堡垒机系统	成功购买CBH实例后，获取登录地址登录云堡垒机系统。 admin 是系统第一个可登录用户，用户密码为自定义设置的密码。
创建用户	创建CBH系统用户，一个用户对应一个系统登录帐号。
添加资源	添加资源信息，并纳管资源账户。 <ul style="list-style-type: none">添加资源，可纳管资源包括Linux主机、Windows主机、数据库、应用系统等。添加资源后，可纳管资源账户，实现自动登录资源进行运维管控。

操作步骤	说明
配置运维权限	创建访问控制权限。 策略授权用户访问资源后，用户才有权限登录相应资源，才能对资源进行运维操作。
登录运维资源	授权用户通过CBH系统登录相应资源，不同资源类型可选择不同登录方式。
审计运维会话	在系统Web页面审计用户系统登录和操作，以及审计用户运维会话。

2 步骤一：登录云堡垒机系统

背景介绍

云堡垒机支持Web浏览器、SSH客户端和MSTSC客户端三种登录方式。

- Web浏览器登录：支持系统管理和资源运维功能。建议系统管理员admin或管理人员使用Web浏览器登录进行系统管理和授权审计。
- SSH客户端登录：在不改变用户原来使用SSH客户端习惯的前提下，可对授权资源进行运维管理。运维人员可选择使用SSH客户端直接登录运维资源。
- MSTSC客户端登录：在不改变用户原来使用MSTSC客户端习惯的前提下，可对授权资源进行运维管理。运维人员可选择使用MSTSC客户端直接登录运维资源。

前提条件

- 已购买CBH实例，若从公网登录需要实例已绑定可用的EIP，具体的操作方法请参见[购买云堡垒机](#)。
- 实例的运行状态为“运行”，CBH系统在使用授权期内。
- 已获取登录CBH系统的登录地址，以及登录验证信息。

通过 Web 浏览器登录云堡垒机

步骤1 启动浏览器，在Web地址栏中输入CBH系统登录地址，进入系统登录页面。

登录地址：<https://云堡垒机实例EIP或私网IP>。例如，<https://10.10.10.10>。

📖 说明

- 未绑定EIP时，可通过私网IP登录，需确保用户本地网络与云堡垒机私网网络通畅。
- 受浏览器兼容性限制，当浏览器版本与云堡垒机系统不匹配时，可能导致登录时获取不到验证信息，或登录后页面显示异常，建议使用推荐的浏览器及版本。推荐浏览器，请参见[使用限制](#)。

步骤2 选择登录认证方式，如[图2-1](#)。

图 2-1 云堡垒机系统登录界面



- 系统所有用户可选择配置“手机短信”、“手机令牌”、“USBKey”和“动态令牌”多因子认证，详情请参考[配置多因子认证](#)。
- 配置多因子认证后，“密码登录”方式认证失效。

表 2-1 Web 浏览器登录验证说明

登录方式	登录说明	登录方式配置说明
密码登录	输入云堡垒机系统的用户登录名和密码。	默认登录方式。 “AD域认证”、“RADIUS认证”、“LDAP认证”或“Azure AD认证”用户登录密码为远程服务器用户密码，详情请参见 远程认证配置 。
手机短信	输入云堡垒机系统的用户登录名和密码，单击“获取验证码”，并输入短信验证码。	需要已经为用户帐号配置可用手机号码。
手机令牌	输入云堡垒机系统的用户登录名和密码，并输入手机令牌的动态验证码（每隔一段时间就会变化）。 说明 需确保用户登录系统时间与手机时间一致，精确到秒，否则会提示验证码错误。	需用户先绑定手机令牌，再由管理员配置多因子认证，否则用户无法登录系统，详情请参考 绑定手机令牌 。
USBKey	插入并选择已签发过的USBKey，并输入对应的PIN码。	需已为用户签发USBKey，详情请参考 签发USBKey 。
动态令牌	输入云堡垒机系统的用户登录名和密码，并输入动态令牌的动态口令（每隔一段时间就会变化）。	需已为用户签发动态令牌，详情请参考 签发动态令牌 。

步骤3 单击“登录”，成功登录云堡垒机系统进行管理和运维操作。

📖 说明

- 系统管理员admin为CBH系统第一个可登录用户，拥有系统最高操作权限，且无法更改权限配置，请妥善保管帐号信息。
- 在首次登录系统成功后，请**所有用户**按照系统提示修改密码和绑定手机号码，否则无法进入系统运行页面。登录系统后，可在个人中心修改用户基本信息。

----结束

通过 SSH 客户端登录云堡垒机

用户获取资源运维权限后，可通过SSH客户端直接登录进行运维操作。

- 支持使用SSH客户端运维的资源，包括SSH、TELNET和Rlogin协议类型主机资源。
- 推荐使用客户端SecureCRT 8.0及以上版本、Xshell 5及以上版本。

步骤1 打开本地SSH客户端工具，选择“文件 > 新建”，新建用户会话。

步骤2 配置会话用户连接。

- 方式一

在新建会话弹出框，选择协议类型，输入系统登录IP地址、端口号（2222），单击“确认”。再输入系统用户登录名，单击“连接”，连接会话。

- 方式二

在新的空白会话窗口，执行登录命令：**协议类型 用户登录名@系统登录IP 端口**，例如执行ssh admin@10.10.10.10 2222。

- 方式三

在正在运行的Linux主机会话窗口，执行登录命令：**协议类型 用户登录名@系统登录IP -p 端口**，例如执行ssh admin@10.10.10.10 -p 2222。

步骤3 用户身份验证。

根据命令提示，在新建会话窗口，输入用户身份验证信息。

SSH客户端登录认证支持“密码登录”、“公钥登录”、“手机短信”、“手机令牌”和“动态令牌”方式。其中“手机短信”、“手机令牌”和“动态令牌”方式，需配置用户多因子认证，详情请参考[配置多因子认证](#)。

表 2-2 SSH 客户端登录验证说明

登录方式	登录说明	登录方式配置说明
密码登录	输入云堡垒机系统的用户密码。	默认登录方式。 “AD域认证”、“RADIUS认证”、“LDAP认证”或“Azure AD认证” 用户登录密码为远程服务器用户密码，详情请参考 配置多因子认证 。

登录方式	登录说明	登录方式配置说明
公钥登录	输入用于验证登录的私钥和私钥密码，登录验证成功后，再次登录时，该用户在SSH客户端可以免密登录。	用户需要先生成用于验证登录的公私钥对，并在云堡垒机系统内的“个人中心”处将SSH公钥添加到云堡垒机系统中，具体的操作请参见 添加SSH公钥 。
手机短信	“密码登录”或“公钥登录”验证成功后，选择“短信验证码”方式，输入手机短信验证码。	需已为用户帐号配置可用手机号码。
手机令牌	“密码登录”或“公钥登录”验证成功后，选择“手机令牌OTP”方式，输入手机令牌验证码。 说明 需确保用户登录系统时间与手机时间一致，精确到秒，否则会提示验证码错误。	需用户先绑定手机令牌，再由管理员配置多因子认证，否则用户无法登录系统，详情请参考 绑定手机令牌 。
动态令牌	“密码登录”或“公钥登录”验证成功后，选择“动态令牌OTP”方式，输入动态令牌验证码。	需已为用户签发动态令牌，详情请参考 签发动态令牌 。

步骤4 登录到云堡垒机系统，可查看系统简要信息，并运维已授权的资源。

📖 说明

除了使用云堡垒机用户密码直接登录外，还支持使用API方式登录云堡垒机指定的资源账户。在登录的用户窗口，输入**用户登录名@资源账户名@主机IP地址:主机端口**，例如 admin@root@192.0.0.0:22。

---结束

通过 MSTSC 客户端登录云堡垒机

用户获取资源运维权限后，可通过MSTSC客户端直接登录进行运维操作。

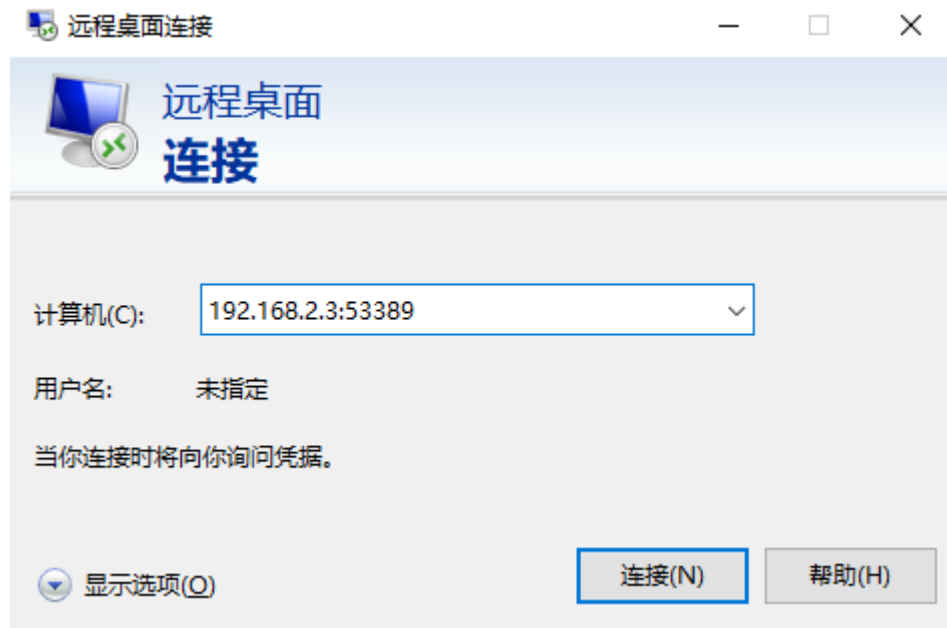
步骤1 打开本地远程桌面连接（MSTSC）工具。

图 2-2 打开远程桌面连接



步骤2 在弹出的对话框中，“计算机”列，输入“堡垒机IP:53389”。

图 2-3 配置计算机



步骤3 单击“连接”，在登录页面完成登录。

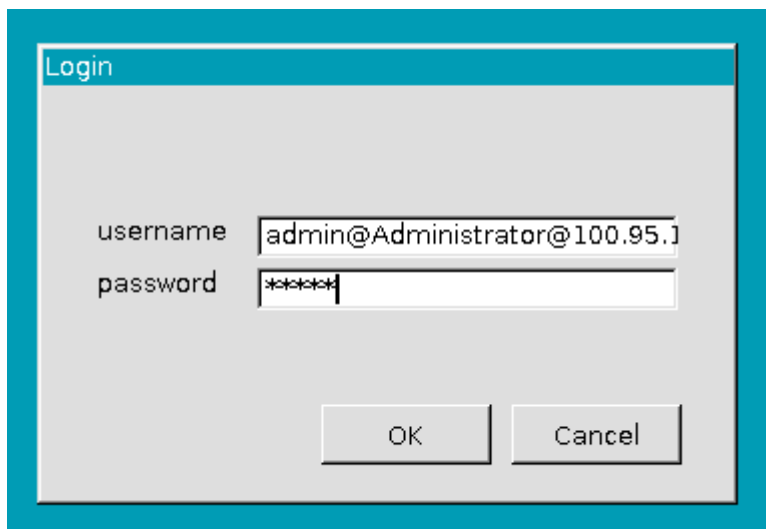
- username: **堡垒机用户登录名@Windows主机资源账户名@Windows主机资源IP:Windows远程端口 (默认3389)**，例如 admin@Administrator@192.168.1.1:3389。

📖 说明

“Windows主机资源账户名”必须是已添加到堡垒机中的资源账户，且登录方式是“自动登录”，否则无法识别Windows主机资源账户，且无法生成运维审计文件。不支持实时会话运维。

- password: 输入当前堡垒机的用户密码。

图 2-4 Login



----结束

3 步骤二：创建系统用户

背景介绍

在使用云堡垒机进行系统管理和运维前，管理人员需要在CBH系统中创建系统用户，为用户分配不同系统角色。

根据角色系统权限的不同，用户拥有不同的系统操作和访问权限，新创建的用户登录系统，即可访问角色权限内模块。

仅admin拥有管理系统角色的权限。

操作步骤

表 3-1 不同创建方式

创建方式	说明
新建单个用户	单个用户仅能逐一创建，适用于创建单个管理员用户。
Excel文件批量导入用户	按照Excel模板要求配置用户信息，再导入系统。 批量添加用户，适用于批量创建运维用户。
同步AD域用户	同步AD域服务器的用户。 同步成功后，使用AD域用户帐号和密码登录CBH系统，AD域服务器同时提供认证服务。

配置说明

表 3-2 用户信息说明

参数	说明
登录名	自定义登录系统的用户名。 创建后不可修改，且系统内“登录名”唯一不能重复。

参数	说明
认证类型	选择登录系统的认证方式。 <ul style="list-style-type: none">● 本地：系统默认认证方式，即通过系统自身的帐号管理系统进行身份认证。● AD域：通过Windows AD域服务器对用户进行身份认证。● LDAP：通过LDAP协议，由第三方认证服务器对用户进行身份认证。● RADIUS：通过RADIUS协议，由第三方认证服务器对用户进行身份认证。● Azure AD：基于SAML配置，由Azure平台对登录用户进行身份认证。
密码/确认密码	用户登录系统的密码。可自定义生成密码，也可随机生成密码。
姓名	自定义用户姓名，便于区分不同的用户。
手机	用户系统预留手机号码。可通过手机短信验证登录身份或找回密码。
邮箱	用户系统预留邮箱地址。可通过邮箱收取系统消息通知。
角色	选择用户的角色，一个用户仅能选择一个角色。 仅 admin 是可自定义角色或编辑默认角色的权限范围。 缺省情况下，系统角色包括部门管理员、策略管理员、审计管理员和运维员。 <ul style="list-style-type: none">● 部门管理员：负责部门系统管理，除“用户管理”和“角色管理”模块之外，部门管理员拥有其他全部模块的配置权限。● 策略管理员：负责策略权限的配置，拥有“用户组管理”、“资源组管理”和“访问策略管理”等模块的配置权限。● 审计管理员：负责系统和运维数据的审计，拥有“实时会话”、“历史会话”和“系统日志”等模块的配置权限。● 运维员：系统普通用户和资源操作人员，拥有“主机运维”、“应用运维”和“授权工单”模块的操作访问权限。
所属部门	选择用户所属部门组织。
用户描述	（可选）对用户情况的简要描述。

4 步骤三：添加系统资源

背景说明

云堡垒机系统集中管理云资源，主要包括管理资源账户和运维权限管理。为实现统一管理资源，需添加资源到系统。

一个主机或应用资源可能有多个登录主机或应用的账户。CBH系统纳管主机或应用的账户（资源账户）后，无需反复输入账户和密码，通过登录资源账户，自动登录资源进行运维管控。

系统默认资源账户Empty，登录Empty资源账户时需手动输入主机账户和对应密码。

前提条件

- 主机与CBH网络通畅，才能从云平台导入和自动发现主机资源。
- 添加应用资源前，需先添加应用发布服务器到CBH系统，可[添加单个](#)或[批量导入](#)应用发布服务器。

操作步骤

表 4-1 资源的不同添加方式

资源类型	添加方式	说明
主机资源	添加单个主机资源	逐一添加主机资源。 主机基本信息添加后，可选择添加主机资源账户。 默认生成Empty资源账户。
	Excel文件批量导入主机资源	按照Excel模板要求配置主机基本信息，可选择配置主机账户信息。 录入主机资源账户后，不再生成Empty资源账户。
	从云平台批量导入	选择与CBH网络通畅的云平台，导入云平台主机信息和主机账户信息。 导入主机全部资源账户，且不再生成Empty资源账户。

资源类型	添加方式	说明
	自动发现	通过IP地址或地址段，自动发现与CBH网络通畅的主机。 自动发现主机只能添加主机信息，需另添加主机资源账户。
应用资源	添加单个应用资源	逐一添加应用资源。 应用基本信息添加后，可选择添加应用资源账户。 默认生成 Empty 资源账户。
	Excel文件批量导入应用资源	按照Excel模板要求配置应用基本信息，可选择配置应用账户信息。 录入应用资源账户后，不再生成 Empty 资源账户。

配置说明

系统内**协议类型@主机地址:端口**需唯一，不能重复，即系统纳管的主机资源唯一。

表 4-2 主机资源基本信息说明

参数	说明
主机名称	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	选择主机的协议类型。 专业版 支持协议类型有SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、SQL Server、Oracle、SCP、Rlogin。 标准版 支持协议类型有SSH、RDP、VNC、TELNET、FTP、SFTP、SCP、Rlogin。
主机地址	输入主机与云堡垒机网络通畅的IP地址 <ul style="list-style-type: none"> 选择主机的EIP地址或私有IP地址，建议优先选择可用私有IP地址。 CBH系统默认要求网络接口为主机的IPv4地址。 主机开启IPv6地址，且在CBH系统网络配置开启了IPv6网络接口后，可配置为主机的IPv4或IPv6地址。 说明 <ul style="list-style-type: none"> 因CBH管理同一VPC网络下的主机资源，私有IP根据网络稳定性与就近优势，不受对外安全策略和访问控制策略的限制。建议“主机地址”优先考虑配置同VPC网络下私有IP地址。 主机的EIP为独立的公网IP，对外访问的端口受网络安全限制，可能导致从云堡垒机无法跳转登录到主机。
端口	输入主机的端口号。

参数	说明
系统类型	<p>(可选) 选择主机的操作系统类型或者设备系统类型。</p> <ul style="list-style-type: none"> 默认支持14种系统类型，包括Linux、Windows、Cisco、Huawei、H3C、DPtech、Ruijie、Sugon、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。 详情请参见系统类型说明。
终端速度	Rlogin协议类型主机可选择不同终端速率。
编码	SSH、TELNET协议类型主机可选择运维界面中文编码。 可选择UTF-8、Big5、GB18030。
终端类型	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	<p>(可选) 选择配置“文件管理”、“剪切板”、“X11转发”。</p> <ul style="list-style-type: none"> 文件管理：仅SSH、RDP、VNC协议类型主机可配置。 剪切板：仅RDP协议类型主机可配置。 X11转发：仅SSH协议类型主机可配置。
部门	选择主机所属部门。
标签	(可选) 自定义标签或选择已有标签。
主机描述	(可选) 对主机的简要描述。

表 4-3 应用资源基本信息说明

参数	说明
应用名称	自定义的应用发布名称，系统内“应用名称”不能重复。
应用服务器	选择已创建的应用发布服务器。
所属部门	选择应用所属部门。
应用地址	<p>(可选) 输入有效IP或域名。</p> <ul style="list-style-type: none"> 应用发布为浏览器时，输入网页地址。若地址有对应的端口，则地址为URL:端口号。 应用发布为数据库或客户端时，输入数据库服务器的地址。
应用端口	<p>(可选) 输入应用访问端口。</p> <ul style="list-style-type: none"> 应用发布为数据库时，输入对应数据库访问的端口。 应用发布为除数据库外其他应用时，无需填写。

参数	说明
应用参数	(可选) 输入应用相关参数。 <ul style="list-style-type: none">应用发布为数据库时，输入实例名。应用发布为除数据库外其他应用时，无需填写。
更多选项	(可选) 选择“文件管理”和“剪切板”。
标签	(可选) 自定义标签或选择已有标签。
应用描述	(可选) 对应用发布的简要描述。

5 步骤四：配置运维权限

背景介绍

用户若需通过云堡垒机运维资源，还需配置访问控制策略，关联用户和资源，赋予用户相应资源访问控制权限。

操作步骤

表 5-1 访问控制策略配置说明

步骤	说明
配置策略基本信息	可配置文件传输权限、用户登录IP限制、用户登录时段限制、策略有效期等信息。
关联用户或用户组	<ul style="list-style-type: none">关联用户：赋权给单个系统用户，该用户角色需同时有“主机运维”和“应用运维”模块权限，才能正常获取运维资源权限。关联用户组：批量赋权给整个用户组成员。赋权后，新加入组的用户即刻拥有该访问控制权限。
关联资源账户或账户组	<ul style="list-style-type: none">关联资源账户：授权访问单个资源账户。关联账户组：授权访问整个账户组。授权后，新加入组的资源账户可立即被赋权用户访问。

配置说明

表 5-2 访问控制策略基本信息说明

参数	说明
策略名称	自定义的访问控制策略名称，系统内“策略名称”不能重复。
有效期	（可选）选择策略生效时间和策略的失效时间。

参数	说明
文件传输	<p>(可选) 在运维过程中, 对资源中文件上传和下载权限。</p> <ul style="list-style-type: none"> • 勾选, 允许对资源中文件上传或下载; • 不勾选, 禁止对资源中文件上传或下载。
更多选项	<p>(可选) 选择在运维过程中主机资源的“文件管理”、“RDP剪切板”、“显示水印”权限。</p> <p>说明 SSH和RDP协议对应的设备支持“文件管理”, VNC协议需通过应用发布才支持。Telnet协议对应的设备不支持“文件管理”。</p>
登录时段限制	<p>(可选) 选择用户登录主机的时间段权限。</p>
IP限制	<p>(可选) 输入限制/允许用户“来源IP”访问资源。</p> <ul style="list-style-type: none"> • 选择“黑名单”, 配置相应IP或IP网段, 即限制该IP或IP网段用户登录资源。 • 选择“白名单”, 配置相应IP或IP网段, 即仅允许该IP或IP网段用户登录资源。 • IP地址缺省状态下, 即不限制用户IP登录资源。

6 步骤五：登录资源运维

背景介绍

用户获取资源访问控制权限后，通过系统登录资源进行运维，运维过程被全程监控记录。

运维用户可根据资源类型选择不同登录方式。

操作步骤

表 6-1 不同登录方式说明

登录方式	适用资源
Web浏览器登录	<ul style="list-style-type: none">SSH、RDP、VNC和TELNET协议类型主机资源。全部应用资源。
SSH客户端登录	SSH、TELNET和Rlogin协议类型主机资源。
FTP/SFTP/SCP客户端登录	适用于全部传输协议类型主机资源。 FTP、SFTP和SCP协议类型主机资源。
SSO单点客户端登录	适用于全部数据库类型主机资源。 <ul style="list-style-type: none">MySQL、SQL Server、Oracle和DB2协议类型主机资源。

7 步骤六：审计运维会话

背景介绍

用户获取相应系统权限和运维权限后，可通过云堡垒机登录已授权的资源进行运维操作，以及在系统进行系统数据管理操作。

管理员可在系统Web页面审计用户系统登录和操作，以及审计用户运维会话。

操作步骤

表 7-1 系统和运维审计说明

审计类型	审计内容
实时会话	实时监控当前运维会话，查看运维用户和资源的会话详情，中断有高危风险的会话。
历史会话	<ul style="list-style-type: none">运维会话视频：无需设置，全程录屏记录运维会话操作，可在线播放或下载操作视频。运维会话详情：用户运维会话详情，可在线查看或导出Excel文件。详情内容包括资源会话信息、系统会话信息、运维记录、文件传输、协同会话的详细操作记录。
运维报表	以折线图的形式，从多方面呈现用户运维资源随时间变化的趋势，并可生成运维资源综合分析报告。 主要涵盖内容有“运维时间分布”、“资源访问次数”、“会话时长”、“来源IP访问数”、“会话协同”、“双人授权”、“命令拦截”、“字符命令数”和“传输文件数”。
系统日志	<ul style="list-style-type: none">系统登录日志：用户登录系统的详细记录，可在线查看或导出Excel文件。系统操作日志：用户系统操作的详细记录，可在线查看或导出Excel文件。

审计类型	审计内容
系统报表	以柱状图的形式，从多方面统计用户登录系统和系统操作次数，并可生成系统管理综合分析报告。 主要涵盖内容有“用户控制”、“用户与资源操作”、“用户源IP数”、“用户登录方式”、“异常登录”、“会话控制”和“用户状态”。

A 修订记录

发布日期	修改说明
2022-12-01	第一次正式发布。