云堡垒机

最佳实践

文档版本 11

发布日期 2024-04-15

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 CBH 最佳实践汇总

本文汇总了云堡垒机（CBH）服务的常见应用场景的操作实践，并为每个场景提供详细的方案描述和操作指南，以帮助您使用CBH快速管理资源。

CBH 最佳实践

表 1-1 CBH 最佳实践

分类	相关文档
变更规格	**变更云堡垒机规格**
高危操作的复核审批	**数据库运维高危操作的复核审批**
等保合规	**云堡垒机等保最佳实践**
跨云、跨VPC、线上线下统一运维	**跨云跨VPC线上线下统一运维最佳实践**
事后追溯	**如何使用堡垒机对安全事故进行事后追溯**

Solution as Code 一键式部署类最佳实践

为帮助企业高效上云，华为云Solution as Code萃取丰富上云成功实践，提供一系列基于华为云可快速部署的解决方案，帮助用户降低上云门槛。同时开放完整源码，支持个性化配置，解决方案开箱即用，所见即所得。

表 1-2 Solution as Code 一键式部署类最佳实践汇总

场景类型	一键式部署方案	说明	相关服务
等保	**等保三级解决方案**	该解决方案依托华为云自身安全能力与安全合规生态，为用户提供一站式的等保三级安全解决方案	WAF、HSS、SCM、SA、MTD、CFW、CBH、DBS、CodeArts Inspector

2 变更云堡垒机规格

2.1 变更前必读

应用场景

随着业务量的不断增长，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。

本文档主要针对单机模式云堡垒机的规格变更规格场景，指导用户在华为云上执行变更规格操作，以及变更规格前后的注意事项和操作指导。

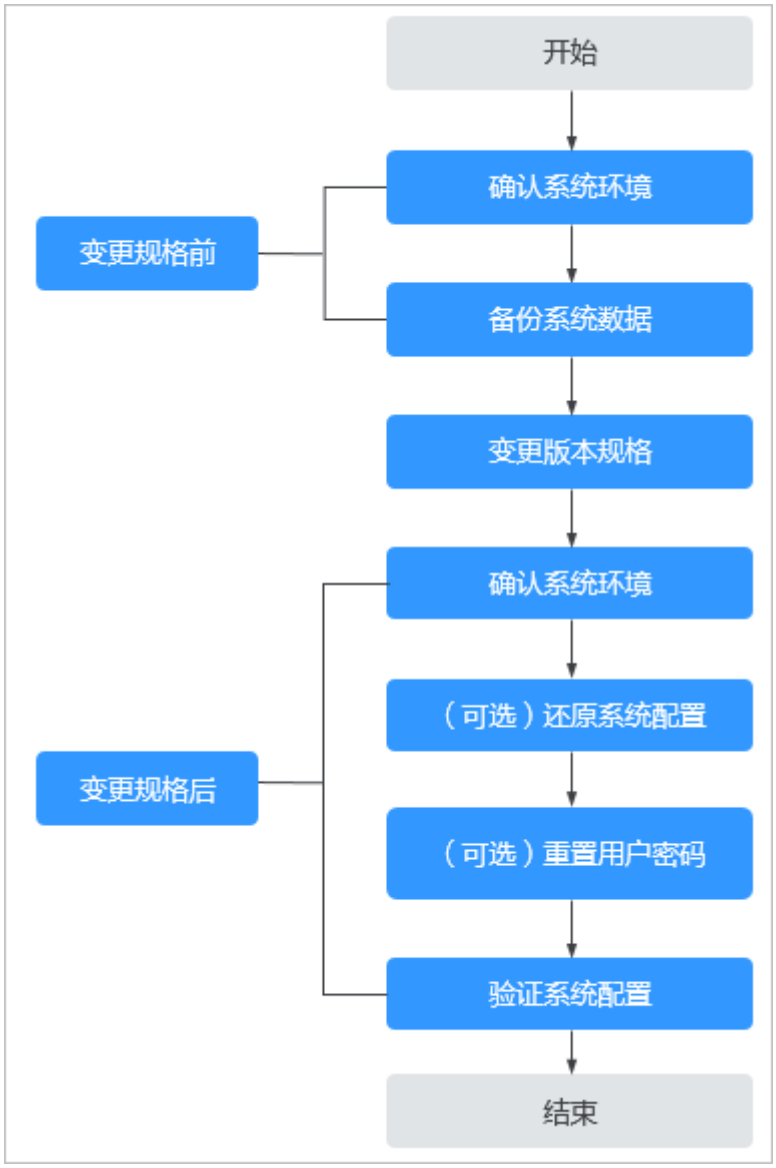
说明

如需变更双机模式的云堡垒机规格，请单击华为云管理控制台右上方的“工单”，填写工单联系技术支持。

变更流程

本文涵盖系统管理员**admin**变更云堡垒机规格的详细过程，包括变更规格前备份系统数据、变更版本规格、变更规格后恢复系统配置，以及验证变更规格后系统配置等过程。

图 2-1 变更规格流程示意图



变更规格限制

变更规格范围涉及系统功能版本和资产规格，详细版本规格请参见**云堡垒机规格版本**。

- 功能版本：仅能从标准版升级到专业版，不能从专业版到标准版。
- 资产规格：涉及资产数、并发数、CPU、内存、数据盘等规格配置。仅能从低规格变更规格到高规格，不能缩容。

说明

- 变更规格不涉及实例绑定的EIP带宽、流量等配置。
- 系统盘默认为100GB，变更规格不影响系统盘，仅涉及数据盘。
- 历史版本仅有标准版功能，如果需变更规格到专业版，请单击华为云管理控制台右上方的“工单”，填写工单反馈云堡垒机历史版本变更规格需求，联系技术支持。
- 变更规则：

  标准版：大于自身资产数量的所有支持的基础版以及大于等于自身资产数量的专业版；

  专业版：大于自身资产数量的所有支持的专业版；

表 2-1 变更支持的版本规格

变更规格前版本规格	变更规格后版本规格
10标准版	10专业版 20标准版、20专业版 50标准版、50专业版 100标准版、100专业版 200标准版、200专业版 500标准版、500专业版 1000标准版、1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
10专业版	20专业版 50专业版 100专业版 200专业版 500专业版 1000专业版 2000专业版 5000专业版 10000专业版
20标准版	20专业版 50标准版、50专业版 100标准版、100专业版 200标准版、200专业版 500标准版、500专业版 1000标准版、1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版

变更规格前版本规格	变更规格后版本规格
20专业版	50专业版 100专业版 200专业版 500专业版 1000专业版 2000专业版 5000专业版 10000专业版
50标准版	50专业版 100标准版、100专业版 200标准版、200专业版 500标准版、500专业版 1000标准版、1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
50专业版	100专业版 200专业版 500专业版 1000专业版 2000专业版 5000专业版 10000专业版
100标准版	100专业版 200标准版、200专业版 500标准版、500专业版 1000标准版、1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
100专业版	200专业版 500专业版 1000专业版 2000专业版 5000专业版 10000专业版

变更规格前版本规格	变更规格后版本规格
200标准版	200专业版 500标准版、500专业版 1000标准版、1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
200专业版	500专业版 1000专业版 2000专业版 5000专业版 10000专业版
500标准版	500专业版 1000标准版、1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
500专业版	1000专业版 2000专业版 5000专业版 10000专业版
1000标准版	1000专业版 2000标准版、2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
1000专业版	2000专业版 5000专业版 10000专业版
2000标准版	2000专业版 5000标准版、5000专业版 10000标准版、10000专业版
2000专业版	5000专业版 10000专业版
5000标准版	5000专业版 10000标准版、10000专业版
5000专业版	10000专业版
10000标准版	10000专业版

变更规格注意事项

- **软件版本要求**

  变更规格到**专业版**，系统软件版本需在V3.2.16.0及以上，否则变更规格后的专业版功能不能生效。

  如果系统软件版本在V3.2.16.0以下，请先**升级软件版本**。

- **系统数据备份与还原**

  变更规格前请务必备份系统重要数据，以免因变更规格失败而导致系统数据丢失。

  变更规格后请根据实际需求将备份数据重新载入系统，还原系统配置。

- **变更规格时间**

  整个变更规格过程包括变更规格前准备、后台变更规格、变更规格后验证，共需60min左右。后台变更规格全程需30min左右，期间CBH系统需要关闭，会导致业务中断。

  为了减少变更规格对系统运行的影响，请尽量选择在业务量较低时进行变更规格操作。

2.2 变更规格前准备

2.2.1 确认变更规格前系统环境

在变更规格前，需确认并记录当前系统版本信息和授权规格，包括“版本号”、“设备系统”、“授权资源数”和“授权资源并发连接数”。

步骤1 登录云堡垒机系统。

步骤2 确认和记录系统版本。

1. 选择“系统 > 关于系统”，查看系统版本信息。

图 2-2 查看系统版本

2. 记录“版本号”和“设备系统”。

说明

“设备系统”为V3.2.16.0及以上，才能变更规格系统到**专业版**，否则请先**升级系统软件版本**。

步骤3 确认和记录授权信息。

1. 选择“系统 > 系统维护 > 授权许可”，查看当前授权规格。

图 2-3 查看授权规格

2. 记录“授权资源数”和“授权资源并发连接数”。

----结束

2.2.2 备份系统数据

为避免因变更规格失败而导致系统数据丢失，变更规格前请务必备份重要系统数据，包括系统配置、资源账户、审计日志等重要数据。

其他系统数据可选择性备份，可备份数据请参见**云堡垒机支持备份哪些系统数据?**

备份系统配置

通过备份和还原系统配置数据，可复用变更规格前系统配置数据。

系统配置文件包括部门、用户、资源、策略、工单、运维、审计和系统模块的全部配置数据。

步骤1 登录云堡垒机系统。

步骤2 选择“系统 > 系统维护 > 配置备份与还原”。

步骤3 单击“新建”创建备份，备份系统配置数据。

图 2-4 创建备份

步骤4 单击“下载”，导出系统配置文件保存于本地。

图 2-5 下载备份文件

----结束

备份资源账户

因不同CBH系统认证密钥的不同，变更规格后可能导致配置文件导入的资源账户不能正常登录。建议备份资源账户信息，以防变更规格失败造成资源账户信息丢失。

资源账户文件包含资源账户的全部数据信息，包括资源账户名称、账户密码、登录方式、特权账户、关联资源名称、资源地址等信息。

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 资源账户”，单击“导出”。

图 2-6 导出资源账户

步骤3 设置资源账户文件的加密密码，加密导出的资源账户文件。

图 2-7 设置文件密码

步骤4 单击“确定”，即可一键下载全部资源账户信息，保存文件于本地。

----结束

备份审计日志

因云堡垒机暂不支持迁移历史审计日志记录，建议在变更规格前备份系统审计日志。

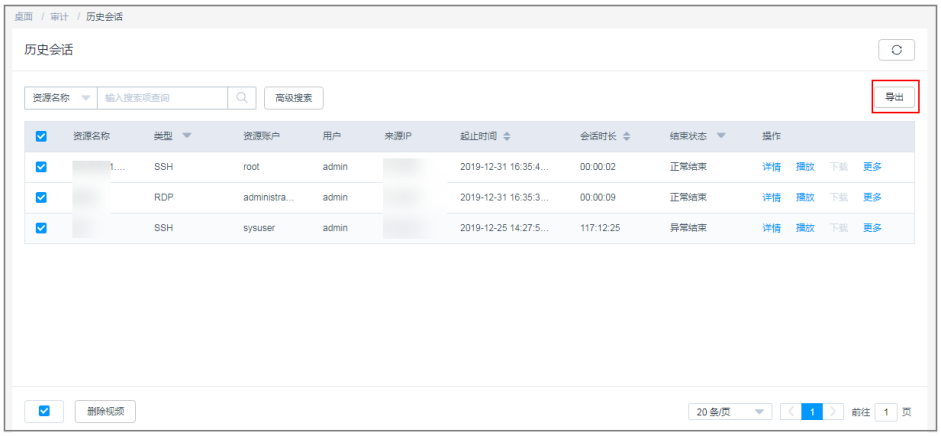
审计日志包括历史会话记录、会话视频、系统登录日志、系统操作日志、改密日志、账户同步日志等。

步骤1 登录云堡垒机系统。

步骤2 导出历史会话日志。

1. 选择“审计 > 历史会话”，进入历史会话页面。
2. 选中所有的历史会话，单击“导出”，导出历史会话的全部文本记录，并将其保存于本地。

图 2-8 导出历史会话



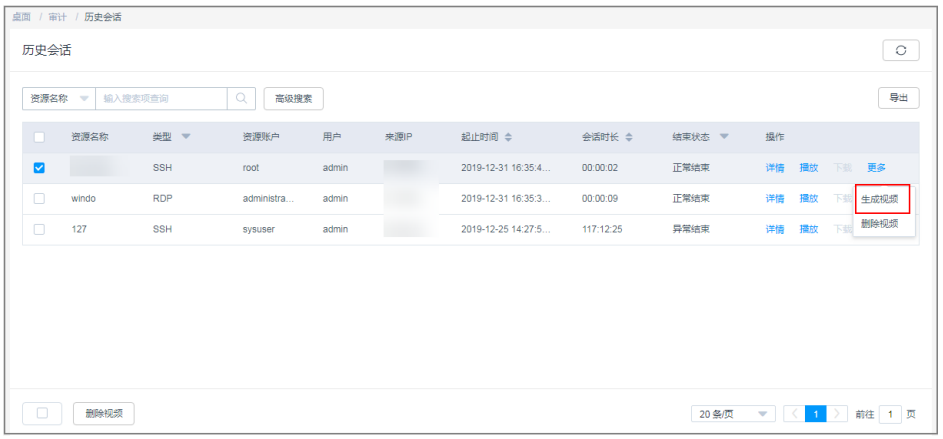
步骤3 下载会话视频。

说明

会话视频文件不支持批量生成和下载，需要逐个操作。

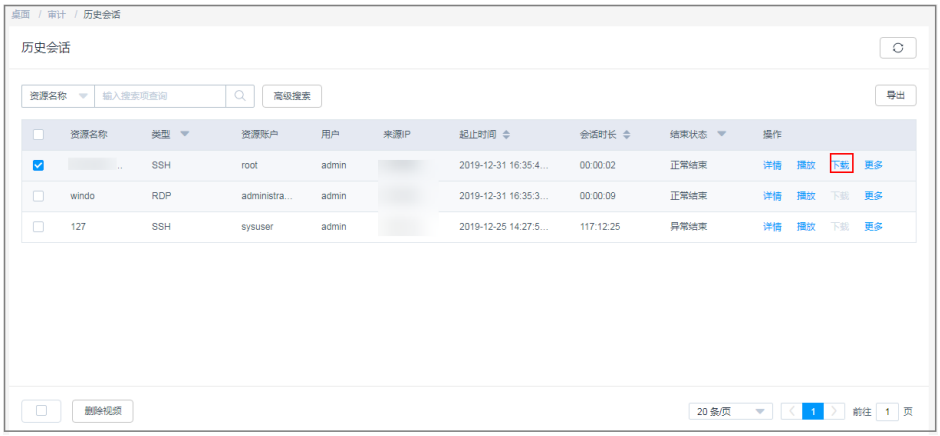
1. 选择“审计 > 历史会话”，进入历史会话页面。
2. 选择历史会话对应“操作”列“更多 > 生成视频”。

图 2-9 生成视频



3. 视频生成后，单击“下载”，将会话视频保存于本地。

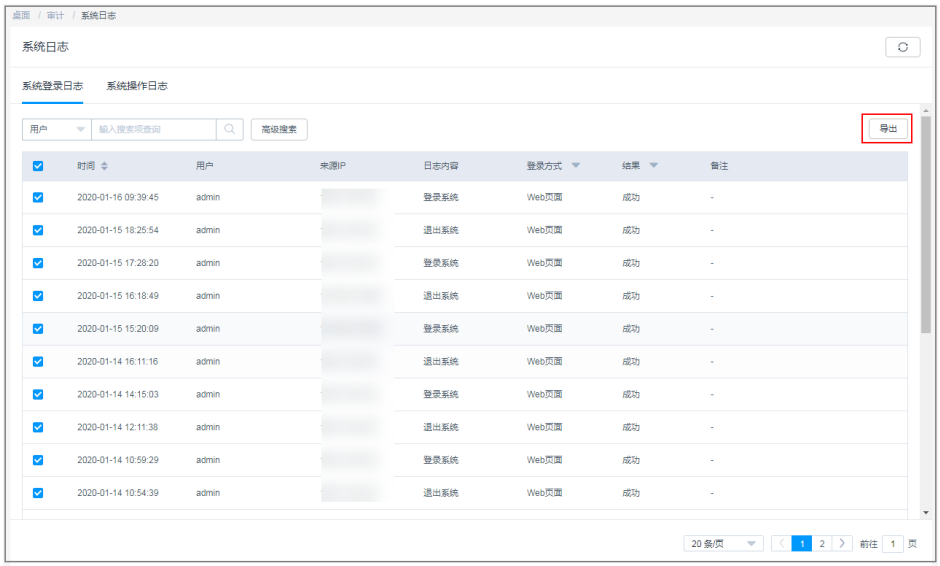
图 2-10 下载视频文件



步骤4 导出系统登录日志。

1. 选择 “审计 > 系统日志 > 系统登录日志”，进入系统日志列表页面。
2. 选中所有的登录日志，单击“导出”，导出系统登录日志的全部文本记录，并将其保存于本地。

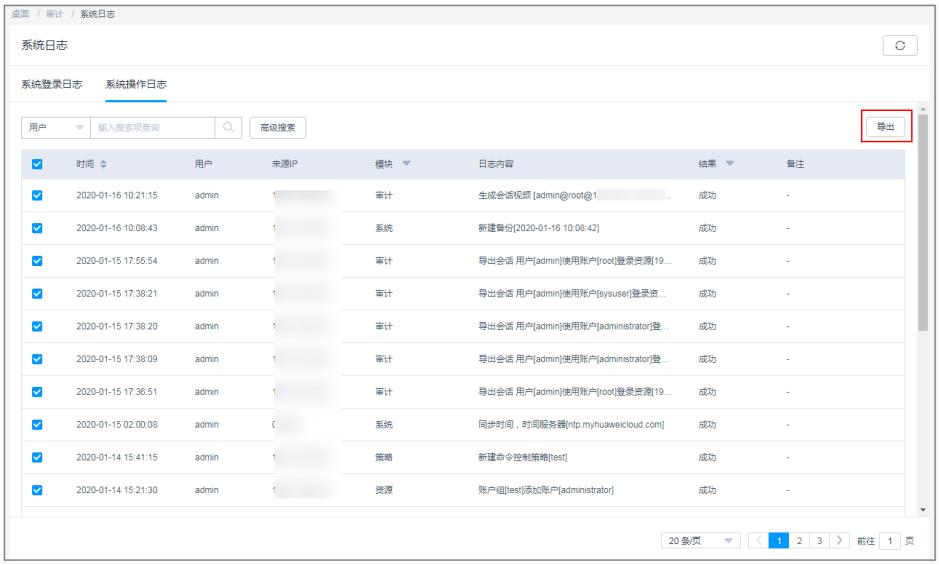
图 2-11 导出系统登录日志



步骤5 导出系统操作日志。

1. 选择“审计 > 系统日志 > 系统操作日志”，进入系统操作日志列表页面。
2. 选中所有的操作日志，单击“导出”，导出系统操作日志的全部文本记录，并将其保存于本地。

图 2-12 导出系统操作日志



----结束

2.3 变更版本规格

前提条件

- 已获取管理控制台的登录账号与密码。
- 已为实例绑定EIP，未绑定EIP的实例不能执行变更规格操作。
- 已**备份系统数据**。
- 已关闭系统，并终止系统所有业务操作。

操作步骤

步骤1 登录管理控制台。

步骤2 如**图2-13**示例，在需变更规格的实例“操作”列，单击“更多 > 变更规格”，开始变更规格版本规格。

图 2-13 实例列表

步骤3 按照变更规格变更要求，选择目标版本规格。

选择目标“性能规格”，单击“立即购买”，进入“订单详情”页面。

步骤4 确认订单并付款。

确认订单无误后，单击“提交订单”。在支付页面，支付变更规格配置款项，完成付款。

步骤5 后台自动变更规格。

成功付款后，后台自动进行变更规格系统操作，整个后台变更规格过程需30min左右，请耐心等待，随时查看状态变化。

后台变更规格过程，实例的运行状态将会由“变更中”变为“正在重启”，系统重启完成实例运行状态变为“正常”。

步骤6 后台变更规格完成。

当实例运行状态转变为“正常”，且“实例规格”信息更新为目标版本规格，即后台变更规格完成。

此时即可正常登录云堡垒机系统，执行变更规格后验证操作。

----结束

2.4 变更规格后验证

2.4.1 确认变更规格后系统环境

变更规格后，请先确认“版本号”和“设备系统”信息，以及确认“授权资源数”和“授权资源并发连接数”是否与目标版本一致。

步骤1 登录云堡垒机系统。

步骤2 确认变更规格后系统版本。

1. 选择“系统 > 关于系统”，查看系统版本信息。
2. 确认变更规格后系统的“版本号”和“设备系统”信息。

图 2-14 查看系统版本

步骤3 确认变更规格后系统授权规格是否为目标规格。

1. 选择“系统 > 系统维护 > 授权许可”，查看授权信息。

图 2-15 查看授权规格

2. 将变更规格后系统的授权信息，与选择目标版本规格进行对比，确认是否一致。
   - 如果一致，则变更规格成功。
   - 如果不一致，需联系技术支持。

----结束

2.4.2 （可选）还原系统配置

后台变更规格成功后，系统资产数、并发数、CPU、数据盘等配置升级，不影响系统数据。

万一变更规格失败导致系统数据丢失，您可以选择导入系统配置、资源账户等备份文件，重新加载还原系统配置。

导入系统配置文件

通过上传备份的系统配置文件，复用变更规格前系统配置数据，还原系统配置。

系统配置文件包括部门、用户、资源、策略、工单、运维、审计和系统模块的全部配置数据。

步骤1 登录云堡垒机系统。

步骤2 选择“系统 > 系统维护 > 配置备份与还原”。

步骤3 在配置还原区域，单击“点击上传”，选择已备份的系统配置文件，并上传。

图 2-16 上传备份文件

步骤4 上传成功后，单击“确定”，完成系统配置文件的导入。

配置文件导入成功后，系统后台读取配置数据还原系统，全程约需5min。如果备份的系统配置数据量大，可能需要时间更长。

----结束

导入资源账户文件

因不同CBH系统认证密钥的不同，变更规格后可能导致配置文件导入的资源账户不能正常登录。为确保资源账户的可用性，建议重新导入备份的资源账户。

资源账户文件包含资源账户的全部数据信息，包括资源账户名称、账户密码、登录方式、特权账户、关联资源名称、资源地址等信息。

步骤1 登录云堡垒机系统。

步骤2 选择“资源 > 资源账户”，进入资源账户列表页面。

步骤3 单击“导入”，进入导入资源账户页面。

图 2-17 资源账户页面

步骤4 单击“点击上传”，选择待迁移的资源账户文件，并上传。

图 2-18 导入账户

步骤5 上传完成后，勾选“更多选项”中的“覆盖已有账户”或“验证账户”。

步骤6 单击“确定”，完成资源账户文件的导入。

----结束

2.4.3 （可选）重置用户密码

变更规格成功后，为确保用户密码的安全性和可用性，加强系统登录安全，建议重置系统用户密码。

密码重置方式可选择批量重置和手动重置两种。

步骤1 登录云堡垒机系统。

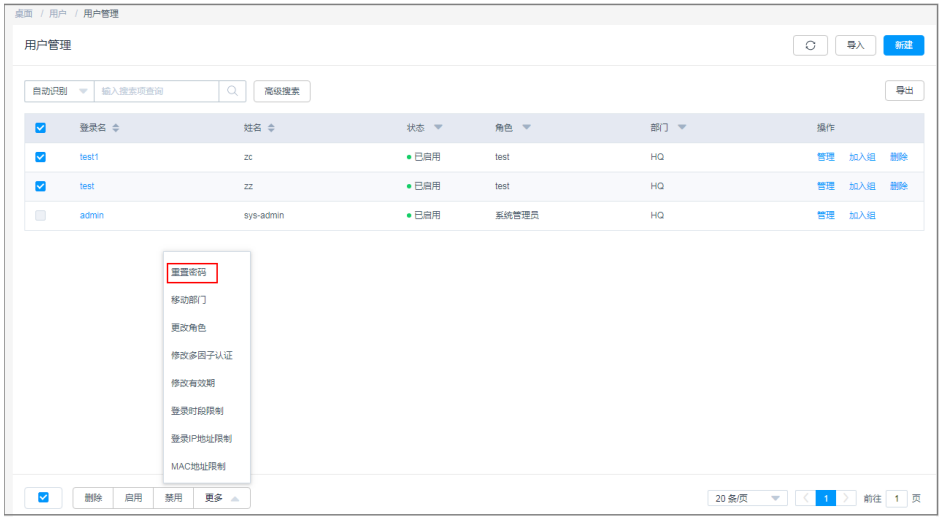
步骤2 选择“用户 > 用户管理”，进入用户列表页面。

- 批量重置，请执行**步骤3**。
- 手动重置，请执行**步骤4**。

步骤3 批量重置，统一生成相同的用户登录密码。

1. 勾选需改密的用户。

图 2-19 重置用户密码



2. 选择“更多 >密码重置”，进入重置密码对话框，设置用户重置密码。

图 2-20 重置用户密码

3. 设置完成后，单击“确定”，完成密码重置。

说明

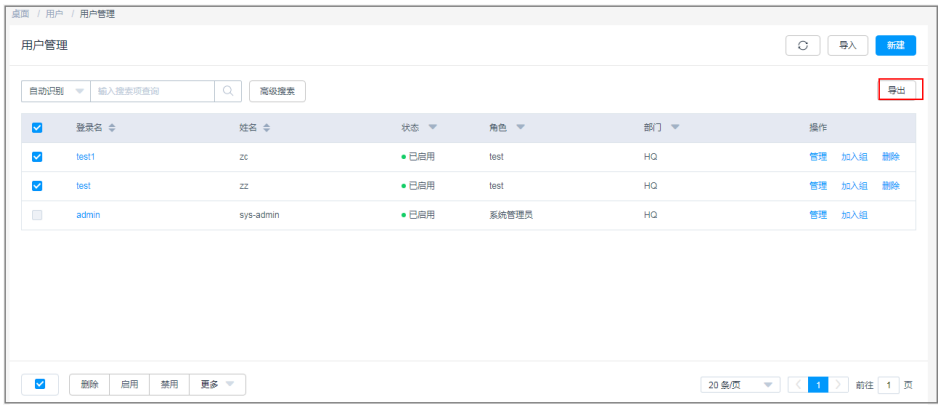
批量重置密码后，所有用户将会用此重置密码登录CBH系统。为了系统账户安全，用户在首次登录系统时，系统会强制用户修改密码。

步骤4 手动重置，可手动设置不同的用户登录密码。

1. 导出用户列表。

   勾选需导出的用户，单击“导出”，导出用户信息。如果不选择，则默认导出全部用户。

图 2-21 导出全部用户



2. 配置用户密码。

   将用户信息文件保存到本地，手动修改“用户登录名”对应的“密码明文”，并保存。

图 2-22 修改密码

	A	B	C	D	E	F	G	H	I	J	K
1	用户登录名	认证类型	密码明文	AD域	用户名称	用户手机号	用户邮箱	用户角色	所属部门	描述	用户组
2		本地认证				18910000000	test@test.com	部门管理员	总部		
3		本地认证				18910000000	test@test.com	部门管理员	总部		
4		本地认证				18910000000	test@test.com	部门管理员	总部		
5		本地认证				18910000000	test@test.com	部门管理员	总部		
6		本地认证				18910000000	test@test.com	部门管理员	总部		
7		本地认证				18910000000	test@test.com	部门管理员	总部		
8		本地认证				18910000000	test@test.com	策略管理员	总部		
9		本地认证				18910000000	test@test.com	部门管理员	总部		
10		本地认证				18910000000	test@test.com	部门管理员	总部		
11		本地认证				18910000000	test@test.com	部门管理员	总部		

3. 导入用户列表。
   a. 单击用户管理页面的“导入”，进入导入用户窗口。

图 2-23 导入用户文件

   b. 单击“点击上传”，选择修改后的用户信息文件并上传。

图 2-24 导入用户

   c. 上传完成后，先选择“更多选项”中的“覆盖已有用户”。
   d. 单击“确定”，用户密码重置成功。

----结束

2.4.4 验证系统配置

变更规格完成后，系统管理员**admin**需逐个选择CBH系统导航树中的以下节点，验证变更规格后系统配置信息是否正确。

待验证系统配置信息，包括部门、用户、资源、策略、工单、审计、运维和系统配置等模块的信息，如表2-2。

表 2-2 验证系统配置

一级节点	二级或三级节点	验证内容
部门	-	验证部门层级数、部门名称、用户数、主机数等配置信息。
用户	用户	验证用户的用户个数、登录名、姓名、状态、角色、归属部门等配置信息。
	用户组	验证用户组个数、名称、组内成员等配置信息。
	角色	验证角色配置信息。
资源	主机管理	验证主机个数、名称、地址、端口、协议、系统类型和账户数等信息。
	应用发布	• 验证应用个数、名称、地址、关联服务器、归属部门等配置信息。 • 验证服务器个数、名称、地址、类型、归属部门等配置信息。
	资源账户	• 验证资源账户个数、名称、关联的资源、地址、端口、归属部门等配置信息。 • 批量选中资源账户，单击“验证”一键验证资源账户状态，确认资源账户是否可正常登录。
	账户组	验证账户组个数、名称、组内成员、成员数等配置信息。
运维	主机标签	验证运维主机的标签个数、名称、加标签主机资源等配置信息。
	应用标签	验证应用发布的标签个数、名称、加标签应用资源等配置信息。
策略	访问控制策略	验证访问控制策略个数、名称、状态、关联用户、关联资源账户等配置信息。
	命令控制策略	• 验证策略个数、名称、执行动作、关联命令集等配置信息。 • 验证命令集个数、名称、命令、参数等配置信息。
	改密策略	验证策略个数、名称、状态、执行方式、改密方式等配置信息。
审计	系统报表	验证报表自动发送配置
	运维报表	验证报表自动发送配置
工单	访问授权工单	验证访问授权工单的工单号、状态和申请时间等基本信息。

一级节点	二级或三级节点	验证内容
系统	安全配置	验证系统登录安全配置信息，包括用户锁定配置、策略密码配置、Web登录配置、SSH客户端登录配置。
	外发配置	验证邮件和短信网关的配置信息。
	认证配置	验证AD域、Radius、LDAP认证等配置信息。
	工单配置	验证工单基本模式、审批流程等配置信息。
	告警配置	验证告警方式、告警等级等配置信息。
	存储配置	验证自动删除功能的配置信息。
	日志备份	验证远程备份至Syslog服务器、远程备份至FTP/SFTP服务器的配置信息。
	配置备份与还原	验证自动备份配置信息。

3 数据库运维高危操作的复核审批

云堡垒机**专业版**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。

本文以管理员**admin_A**授权运维用户**User_A**，针对MySQL数据库资源**RDS_A**高危操作的二次授权为例。

应用场景

云堡垒机（Cloud Bastion Host，CBH），通过设置数据库控制策略，设置预置命令执行策略，动态识别并拦截高危命令（包括删库、修改关键信息、查看敏感信息等），中断数据库运维会话。同时自动生成数据库授权工单，发送给管理员进行二次审批授权。只有管理员审批工单授权执行操作后，运维用户才能执行该高危操作，继续数据库运维会话。

约束限制

目前仅支持二次审核MySQL或Oracle数据库的执行命令。

前提条件

- 已购买**专业版**云堡垒机，且能正常登录云堡垒机系统。
- 云堡垒机所在**安全组**已放开相应数据库访问端口，数据库与云堡垒机之间网络连接畅通。
- 资源**RDS_A**已被纳管为主机运维方式资源，详情请参见**如何创建数据库运维？**。
- 运维用户**User_A**已获取资源**RDS_A**的访问控制权限，详情请参见**创建访问控制策略**。

配置二次审核策略

为实现高危操作的复核审批，需在“数据库控制策略”中预置命令规则，并开启“动态授权”执行方式。

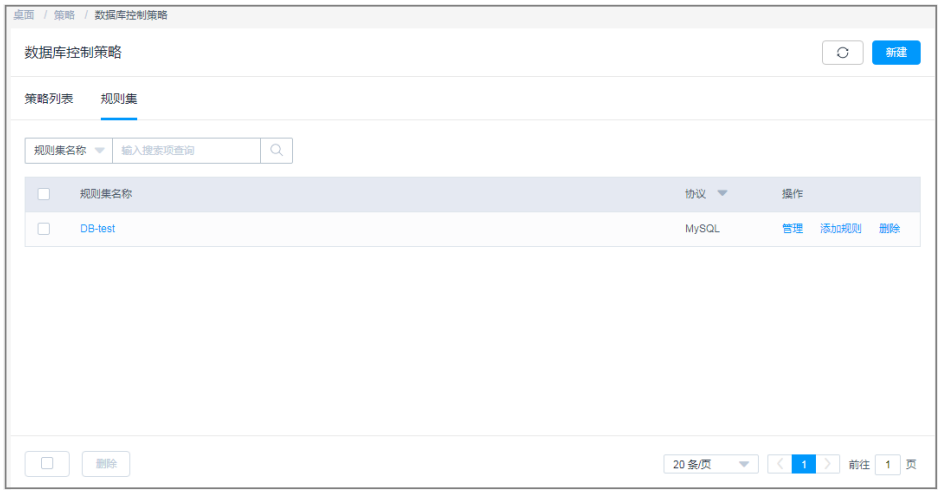
步骤1 **admin_A**登录云堡垒机系统。

步骤2 选择“策略 > 数据库控制策略”，进入数据库控制策略页面。

步骤3 配置数据库规则集，选择预置高危操作命令。

1. 选择“规则集”页签。

图 3-1 规则集管理页面



2. 单击“新建”，创建一个MySQL数据库的规则集。以新建**DB-test**规则集为例。

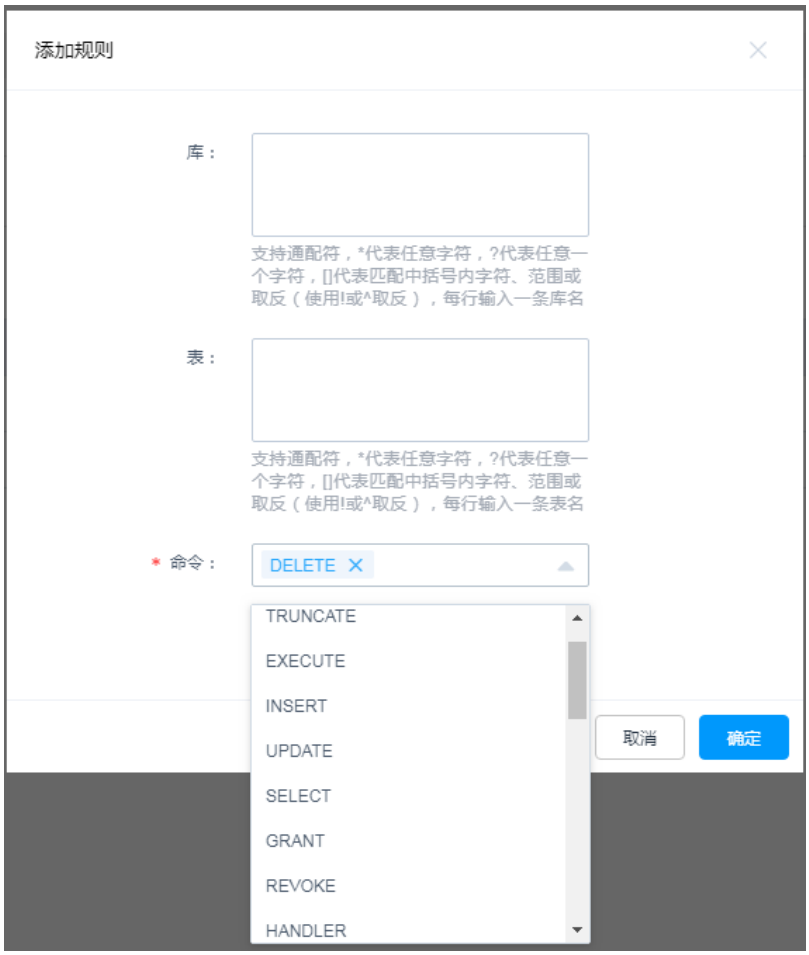
图 3-2 创建规则集

3. 单击“添加规则”，在**DB-test**规则集中添加“库”、“表”或“命令”规则。以添加**DELETE**删除表内容的命令为例。

说明

- “命令”为必填项，至少需选择一个命令，可同时选择多个命令。
- 设置“库”或“表”，表示对数据库中库或表操作的命令限制。
- 未设置“库”或“表”，表示对数据库中全部操作的命令限制。

图 3-3 添加命令规则



步骤4 配置数据库策略。

1. 选择“策略列表”页签。

图 3-4 数据库控制策略管理页面

2. 单击“新建”，创建一个“动态授权”的数据库控制策略。以新建**DB-ACL**策略为例。

图 3-5 配置动态授权

3. 关联规则集**DB-test**。

图 3-6 关联规则集

4. 关联用户**User_A**和关联资源**RDS_A**。

图 3-7 关联用户和资源

----结束

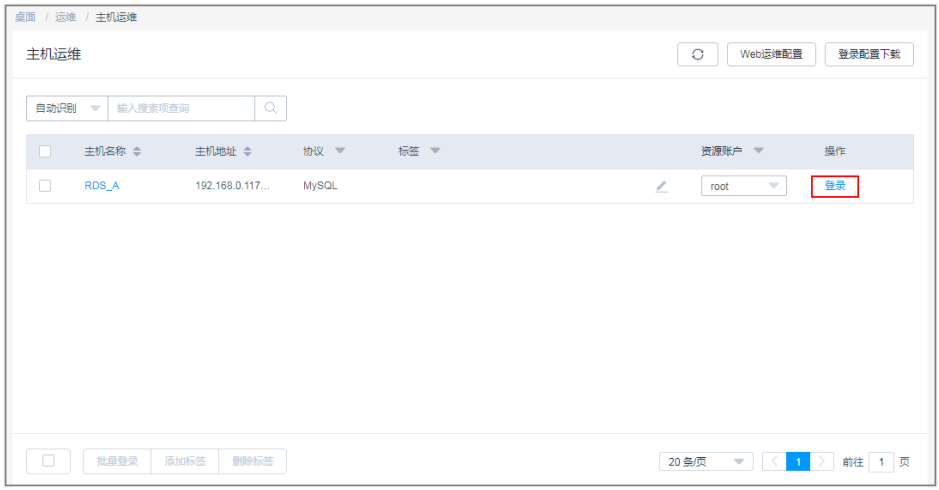
效果验证

运维用户执行高危操作，触发拦截，申请操作权限。管理员通过对高危操作的二次审核，加强对数据库核心资产的管控力度。

步骤1 运维用户**User_A**登录资源**RDS_A**。

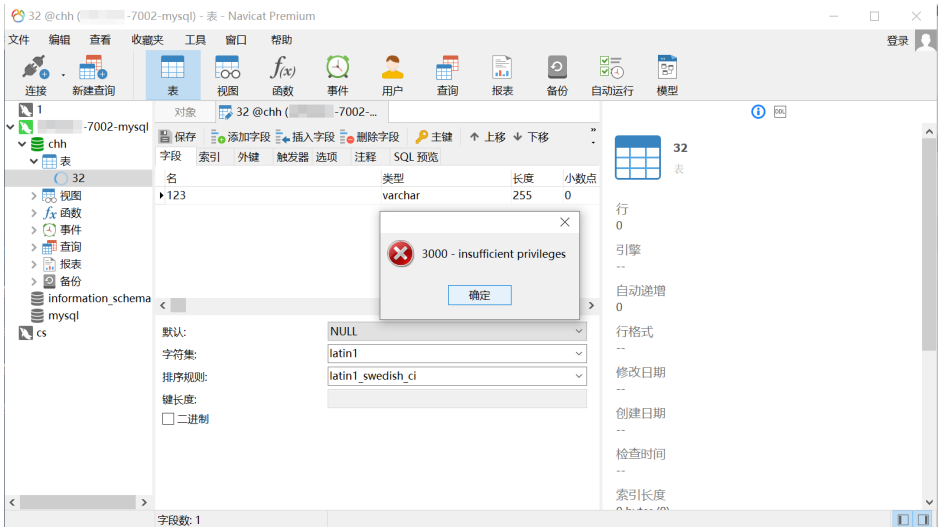
1. 登录云堡垒机系统。
2. 选择“运维 > 主机运维”。
3. 单击“登录”，通过**SSO单点登录**工具调用数据库客户端，登录数据库资源**RDS_A**。

图 3-8 登录数据库资源



步骤2 以调用Navicat客户端登录数据库为例。运维用户**User_A**在资源**RDS_A**中，执行删除表内容操作，自动触发拦截**DELETE**命令，提示无权限删除。

图 3-9 触发拦截



步骤3 运维用户**User_A**提交数据库授权工单，反馈给管理员**admin_A**审批。

1. 运维用户**User_A**登录云堡垒机系统。
2. 选择“工单 > 数据库授权工单”，查看因删除操作被拦截而产生的工单。
3. 单击“提交”，提交对资源**RDS_A**删除操作的授权申请。

图 3-10 提交数据库授权工单

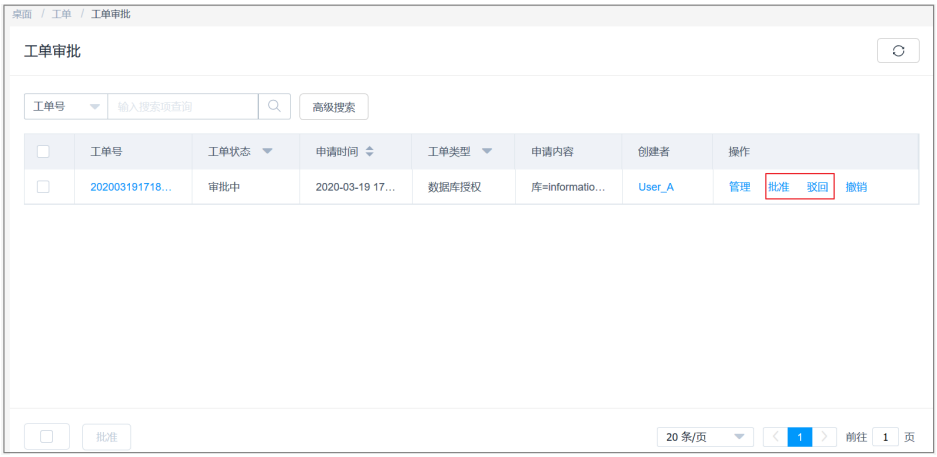
步骤4 管理员**admin_A**审核运维用户**User_A**的运维操作，根据实际情况批准或驳回申请。

1. 管理员**admin_A**登录云堡垒机系统。
2. 选择“工单 > 工单审批”，审核**User_A**数据库授权工单。
3. 单击“批准”或“驳回”，审批工单。

说明

仅管理员“批准”工单后，运维用户才能继续执行被拦截的高危操作。

图 3-11 审批工单



----结束

4 云堡垒机等保最佳实践

为助力企业通过等保合规测评，本文为您介绍云堡垒机各项功能与等保相关条款的对应关系，以便您有针对性地提供佐证材料。

等保三级相关条款

该最佳实践将主要聚焦于满足以下等保条例的考察内容：

- 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
- 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
- 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
- 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现
- 应对登录的用户分配账户和权限；
- 应重命名或删除默认账户，修改默认账户的默认口令；
- 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- 应授予管理用户所需的最小权限，实现管理用户的权限分离；
- 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

前提条件

已购买标准版及以上版本堡垒机，并已完成堡垒机配置。

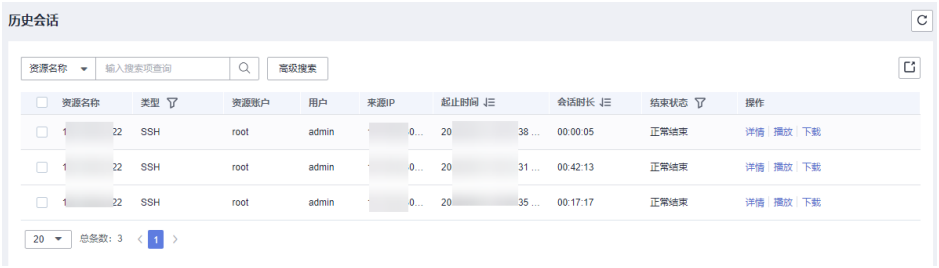
安全区域边界：安全审计

- 等保条例：**应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；**

  本条款主要考察：是否有进行安全审计。云堡垒机支持对云服务器运维操作进行监控和审计。

  - 使用有审计模块权限的账号登录云堡垒机，单击“审计 > 历史会话”，进入“历史会话”页面。

    图 4-1 查看历史会话

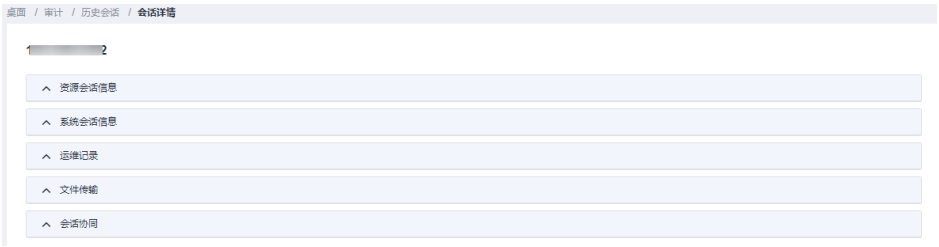
  - 在历史会话页面可分别查看资源会话信息、系统会话信息、运维操作记录、文件传输记录、会话协同记录等。具体操作详见**云堡垒机历史会话**。

- 等保条例：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

  本条款主要考察：日志是否按照要求进行记录。

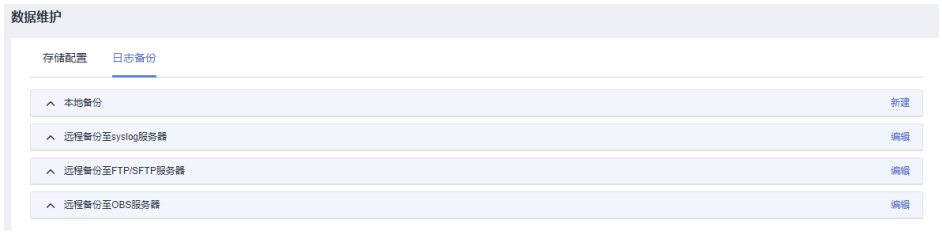
  - 使用管理员账号登录云堡垒机，单击“审计 > 历史会话审计”，进入“历史会话”页面。
  - 主要包含资源名称、类型、主机IP、资源账户、起止时间、会话时长、会话大小、操作用户、操作用户来源IP、操作用户来源MAC、登录方式、运维记录、文件传输记录、会话协同记录等信息。具体操作详见**云堡垒机历史会话**。

    图 4-2 查看历史会话信息

- 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
  - 使用管理员账号登录云堡垒机，单击“系统 > 数据维护”，单击“日志备份”，进入“日志备份”页面。
  - 在“日志备份”页面，可以创建、查看日志备份，支持系统登录日志、资源登录日志、命令操作日志、文件操作日志、双人授权日志。也支持备份至Syslog服务器、FTP/SFTP服务器和OBS桶。具体操作详见**云堡垒机创建数据备份**。

图 4-3 创建数据备份



- 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；

  本条款主要考察：是否能够对远程访问的用户行为进行审计与数据分析。具体详见**云堡垒机运维审计**。

安全计算环境：身份鉴别

- 等保条例：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

  本条款主要考察如下三点：

  a. 是否对登录用户进行身份识别和鉴别使用浏览器访问堡垒机页面，证明需要对用户身份进行鉴别之后才可正常使用产品功能。

  图 4-4 云堡垒机登录界面

  b. 身份标识是否具有唯一性：每名用户创建必须填写姓名、手机号、邮箱及角色，并且一名用户只能配置一个角色。详见：**云堡垒机创建用户**。

图 4-5 创建用户

c. 身份鉴别信息是否具有复杂度要求并定期更换：云堡垒机支持“手动执行”、“定时执行”、“周期执行”三种改密执行方式，还支持“生成不同密码”、“生成相同密码”、“指定相同密码”三种改密方式。具体操作详见**云堡垒机改密策略**。

图 4-6 改密策略

- 等保条例：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现;

  云堡垒机采用多因子认证的登录方式，具体登录认证的方法有：手机短信、手机令牌、USBkey和动态令牌登录四种方式。具体操作详见：**云堡垒机配置多因子认证**。

图 4-7 配置多因子认证

- 等保条例：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

  云堡垒机可配置用户登录安全锁，可设置锁定方式、锁定时长、可尝试密码次数等。具体操作详见：**云堡垒机配置用户登录安全锁**。

图 4-8 登录安全锁

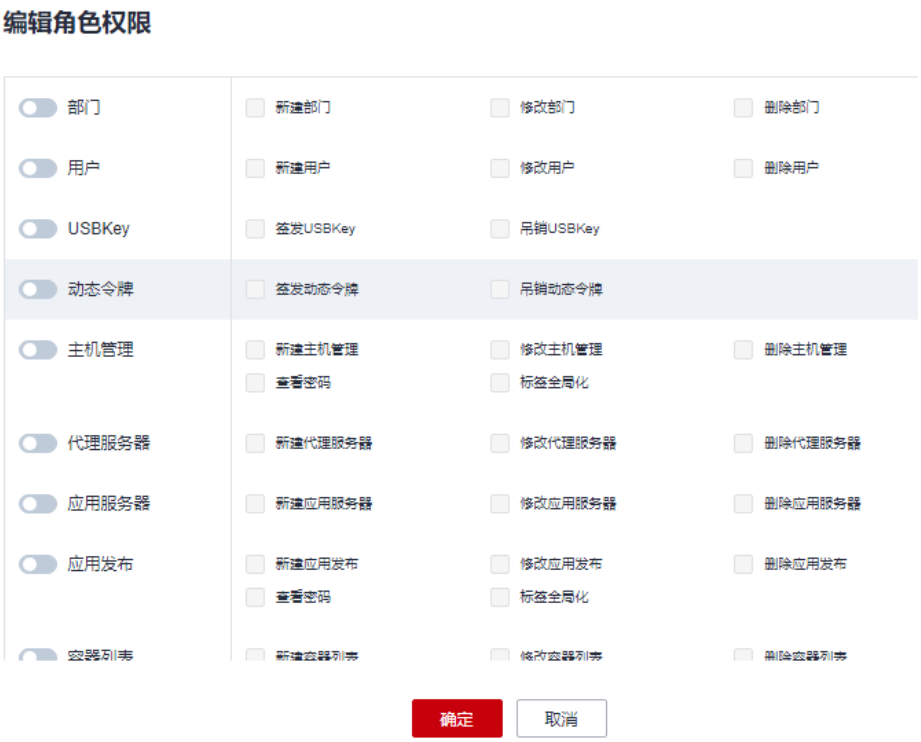
访问控制

- 等保条例：应授予管理用户所需的最小权限，实现管理用户的权限分离；

  云堡垒机支持对用户的操作权限进行限制，分别为三大类：访问控制策略、命令控制策略和数据库控制策略。

  a. 云堡垒机可以对登录用户角色的一些操作权限进行控制，比如您可以对运维主管的账号授予删除和修改代理服务器的权限。

图 4-9 角色权限细粒度



b. 您可以对各个账户进行访问控制，具体可细分到文件管理、上行剪切板、下行剪切板、显示水印、控制登录时间和上传下载文件，并且可以对登录的角色进行IP的黑白名单限制。

图 4-10 访问控制策略

- 等保条例：应对登录的用户分配账户和权限；

  云堡垒机支持对用户进行角色分配和用户组分配，具体操作详见：云堡垒机用户角色管理和云堡垒机用户组管理。

  对于长期不登录或过期的账户，应及时删除。云堡垒机可以设定僵尸用户判定时间，超过此时间的账户就会被禁用。

图 4-11 僵尸用户判定规则设定

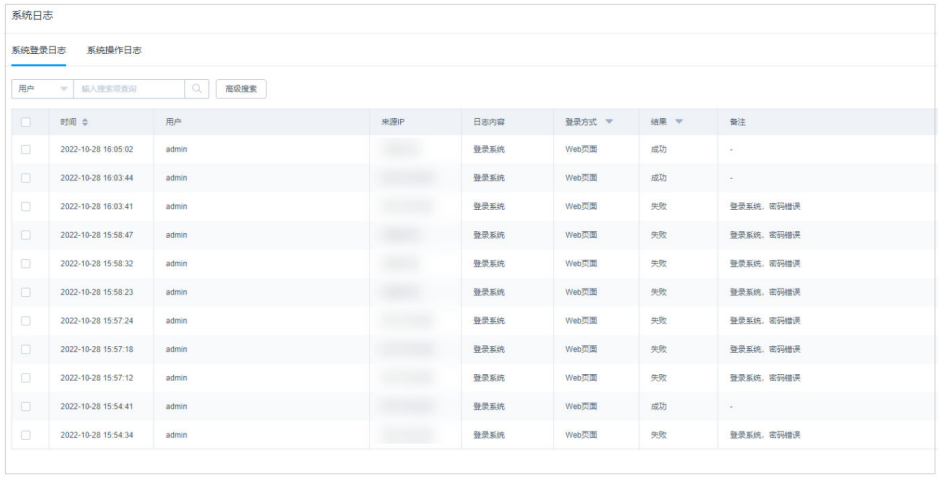
安全审计

- 等保条例：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

  云堡垒机支持查看实时会话、查看历史会话及查看查看系统日志的功能。

您可以在系统日志中查看系统登录日志，具体可细分为登录时间、登录用户、来源IP、日志内容、登录方式、登录结果和备注等内容。

图 4-12 系统登录日志



- 等保条例：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

  可以在系统操作日志中详细查看每个账号对堡垒机做了哪些操作，具体记录到用户、时间、来源IP、模块、日志内容、结果。

图 4-13 系统操作日志

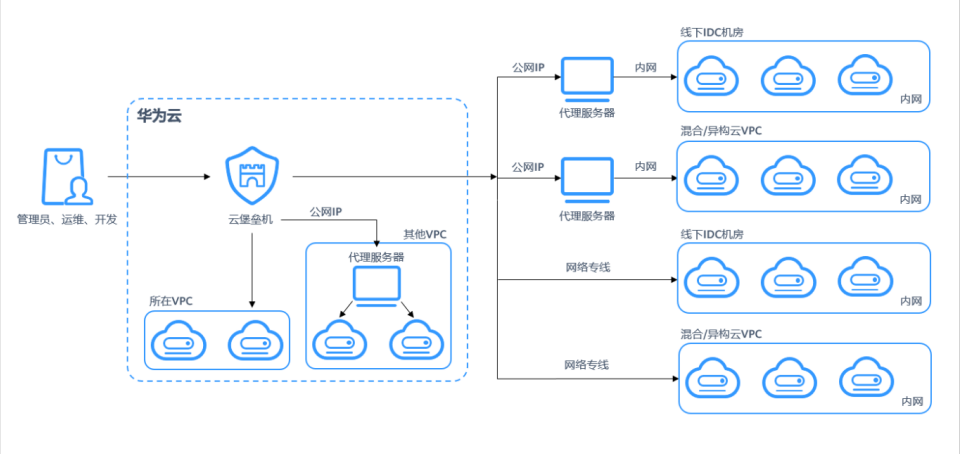
5 跨云跨 VPC 线上线下统一运维最佳实践

应用场景

针对您的服务器资源分布在跨VPC、线下IDC机房、非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，从而通过云堡垒机统一管理、运维您的各类工作负载。

本文指导您如何在目标网络域配置代理服务器、连通华为云云堡垒机，并实现通过云堡垒机对您跨VPC、跨云、线下的资源进行管理与运维。

图 5-1 跨云跨 VPC 线上线下统一运维示意图



前提条件及准备工作

- 已购买堡垒机并正常使用。
- 已购买弹性云服务器（ECS）并正常使用。
- 已在对端网络域中获取1台服务器作为代理服务器。
- 代理服务器已绑定弹性公网IP，具体操作请详见：**将弹性公网IP绑定至实例**。
- 代理服务器与待纳管服务器网络互通。
- 已下载**最新版本3proxy**压缩包。

设置代理服务器

在需要对跨网络域的服务器进行管理运维前，需要在对端网络域中配置一台网络代理服务器。将该代理服务器与业务服务器通过内网进行互通，再将代理服务器到云堡垒机网络进行互通，即可完成云堡垒机到业务服务器之间跨域的网络互联。

该部分操作是达成堡垒机跨域纳管主机资源的前提。

- **为代理服务器启用网络代理服务**

步骤1 登录代理服务器，进行代理服务器（3proxy）设置。

注意

步骤二至步骤四中的命令，均以CentOS7为例。如需CentOS8代码示例，请参见**CentOS8配置代理示例**。

步骤2 上传3proxy压缩包并解压后，进入对应目录执行以下命令：

bash install.sh

步骤3 输入如下命令，添加3proxy用户

/etc/3proxy/add3proxyuser.sh myuser mypassword

步骤4 重启代理服务3proxy

systemctl restart 3proxy

说明

- socks5代理协议（端口：1080）没有加密功能，如果通过代理服务器运维使用了非加密的协议类型，请务必在安全组设置中禁止非必要的IP访问。
- 如果需要加密传输或数据安全的考量，在选择出入方向规则时建议选择有加密的协议类型：SSH、RDP、SFTP、SCP、Rlogin。

----结束

- **为代理服务器配置安全组规则**

步骤1 进行代理服务器**入方向规则配置**，允许堡垒机访问代理服务器。

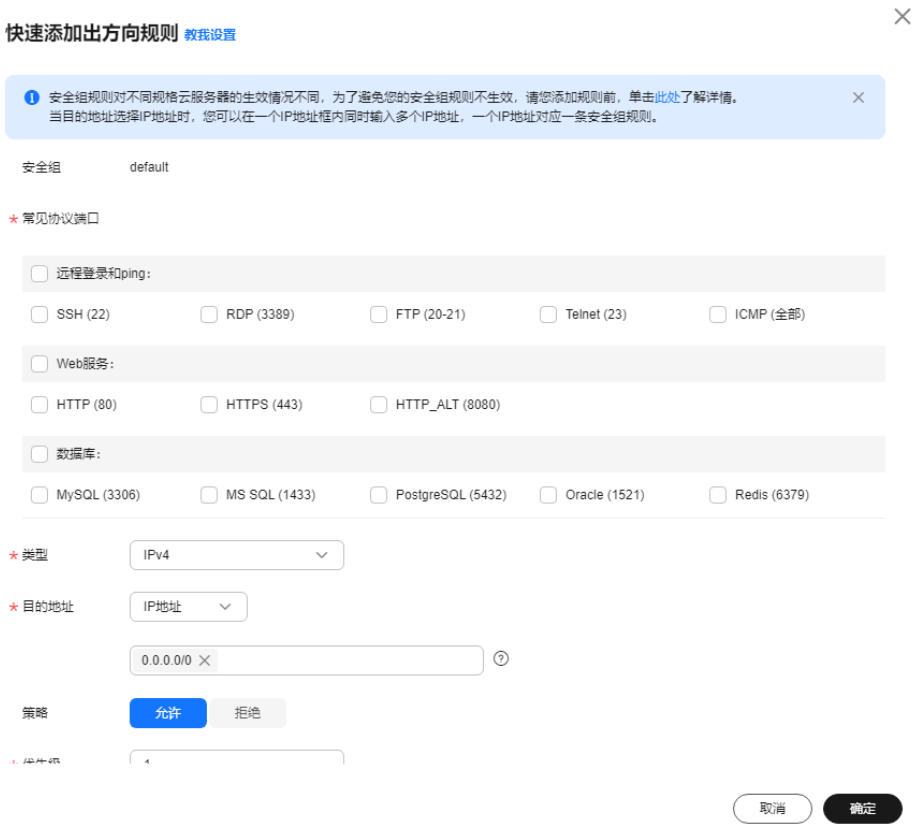
图 5-2 入方向规则配置

说明

- 在“协议端口”中填写socks5代理服务器默认的“1080”端口。
- 在“源地址”中填写堡垒机的IP地址。

步骤2 进行代理服务器出方向规则配置，允许代理服务器访问待纳管的业务服务器。

图 5-3 出方向规则配置



----结束

通过云堡垒机纳管跨域的业务服务器

步骤1 登录“网络控制台”>“访问控制”>“安全组”，进入“安全组”页面，对云堡垒机所在安全组规则进行入方向、出方向配置。

图 5-4 云堡垒入方向规则配置

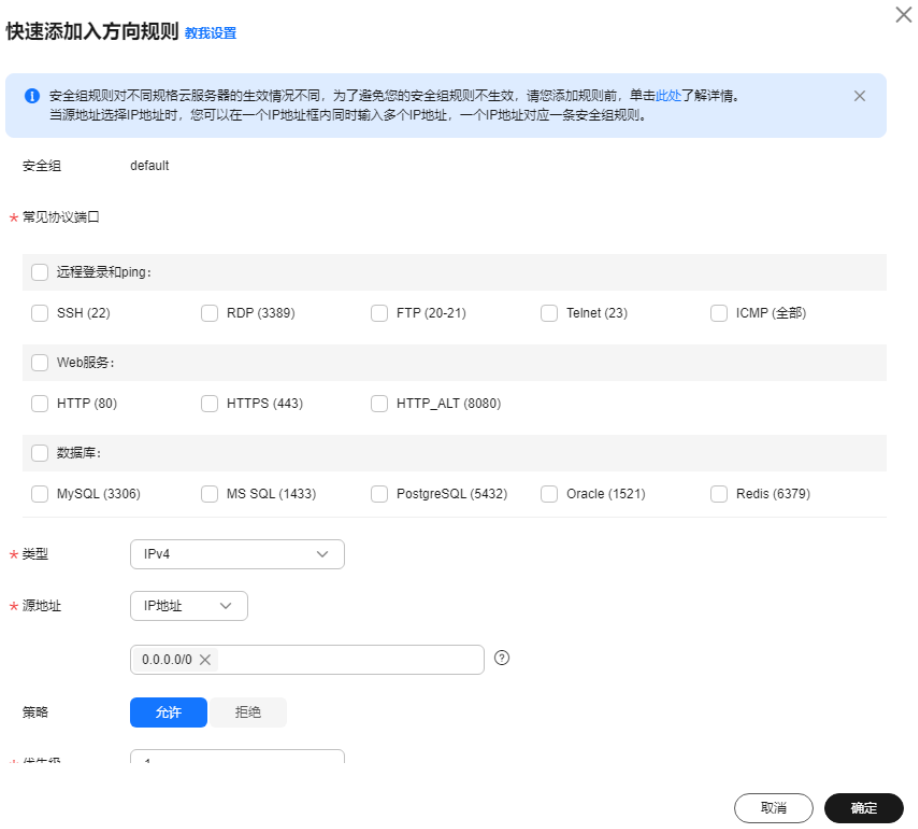


图 5-5 配置云堡垒机出方向规则

步骤2 通过云堡垒机纳管代理服务器。登录云堡垒机系统，添加代理服务器，操作步骤请见**添加主机资源**，在“主机管理”页面选择“代理服务器”，单击“新建”。

图 5-6 新建代理服务器

步骤3 对待纳管的业务服务器所在的安全组入方向规则进行配置，在步骤1中“入方向规则”页面，单击“快速添加规则”。

说明

出方向规则根据您的需要请自行添加配置。

步骤4 通过云堡垒机纳管业务服务器，具体操作步骤请见添加主机资源。

图 5-7 新建主机

----结束

通过上述步骤的操作后，您可以根据云堡垒机自带的主机运维功能跨网络域运维被纳管的主机资源。类似地，可将以上做法推广到混合/异构云、线下IDC等不同网络环境，以实现跨云跨VPC线上线下统一运维。

CentOS8 配置代理示例

步骤1 执行如下命令，安装3proxy软件包

yum install -y epel-release

yum install -y 3proxy

步骤2 执行如下命令，进行极简配置

nscache 65536

timeouts 1 5 30 60 180 1800 15 60

#设置用户名：在users指令后输入您需要设置的用户名，本章节以**test**为例 密码：在CL指令后输入您需要设置的用户名，本章节以**test**为例。

users test:CL:test

daemon

log /var/log/3proxy/3proxy.log

logformat "- +_L%t.%. %N.%p %E %U %C:%c %R:%r %O %I %h %T"

archiver gz /bin/gzip %F

rotate 30

external 0.0.0.0

internal 0.0.0.0

auth strong

allow test

maxconn 20

socks

flush

步骤3 启动服务

systemctl start 3proxy

----结束

6 如何使用堡垒机对安全事故进行事后追溯

随着业务上云并不断发展，云上运维的人数不断增加，这样必然会衍生出一些运维人员操作疏忽而导致的一些安全事故，但由于传统服务器缺少指令监控，操作回放等功能，这样就导致安全事件可追溯性不完善的问题。

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。

简介

本章节介绍了云堡垒机如何通过会话审计功能对安全事件进行追溯调查，完成安全事件的责任界定。

前提条件

已购买云堡垒机，并且使用有审计模块权限的账号登录云堡垒机

对历史会话进行审计

步骤1 登录控制台。进入“历史会话”页面，具体操作步骤详见**查看历史会话**。

步骤2 根据您业务出现安全问题的一些信息，在“高级搜索框”中输入相关信息进行检索。

图 6-1 高级搜索

步骤3 根据搜索完后的结果，在“操作”列单击“详情”，进入“会话详情”页面，对历史操作指令、文件传输情况进行排查。

----结束

根据上述步骤您就可以根据操作指令的情况，排查出是哪个步骤出现了问题，为您的事件追溯提供了便利性。当然您也可以使用会话回放功能，通过播放运维视频，来查看具体的操作情况，具体操作步骤请参见**管理会话视频**。

须知

华为云堡垒机还为您提供实时会话监控功能，让您可以实时查看高危操作的运维界面，如果出现危险指令可立即切断运维人员的操作，确保业务的安全。具体请参见**云堡垒机实时会话**章节。

