云堡垒机

最佳实践

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。

目 录

1 变更云堡垒机规格

1.1 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。

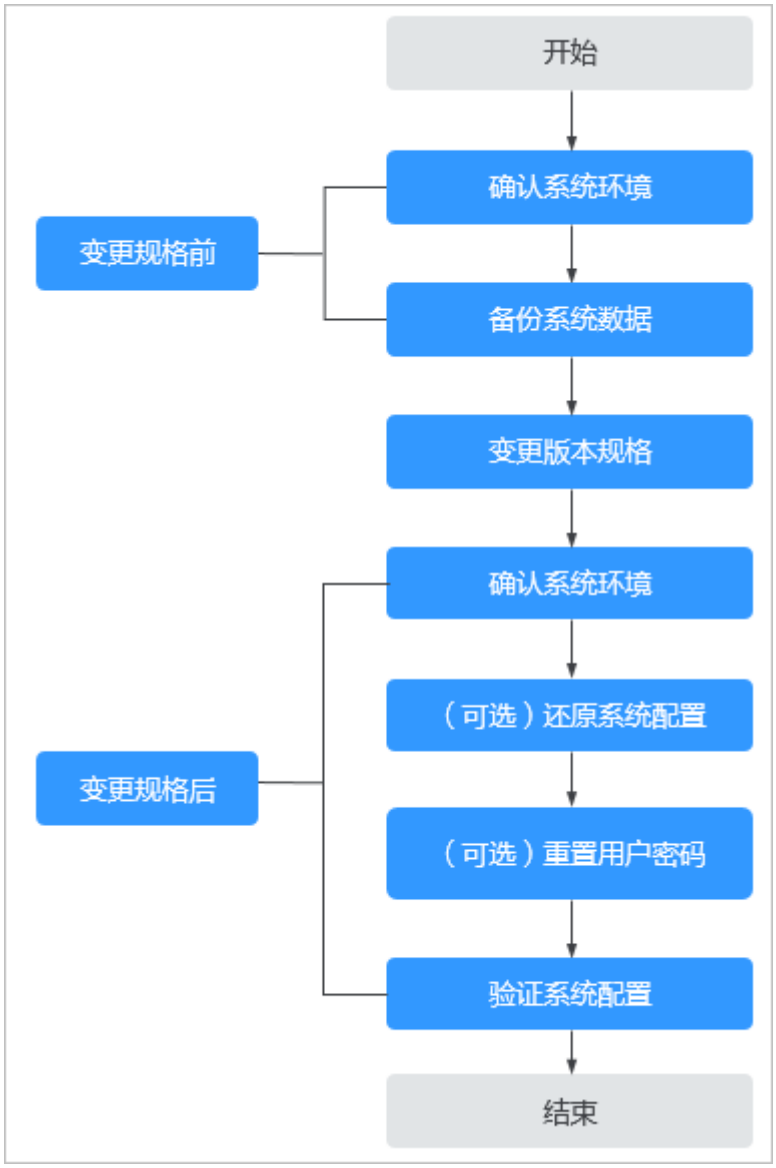
说明

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 1-1 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。

- 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，若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。

表 1-1 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
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 5000标准版、5000专业版
100专业版	200专业版 500专业版 1000专业版 5000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 5000标准版、5000专业版
200专业版	500专业版 1000专业版 5000专业版
500标准版	500专业版 1000标准版、1000专业版 5000标准版、5000专业版
500专业版	1000专业版 5000专业版
1000标准版	1000专业版 5000标准版、5000专业版
1000专业版	5000专业版
5000标准版	5000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。

  若系统软件版本在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。

1.2 变更规格前准备

1.2.1 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 1-2 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 1-3 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

1.2.2 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。

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 1-4 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 1-5 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 1-6 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 1-7 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。

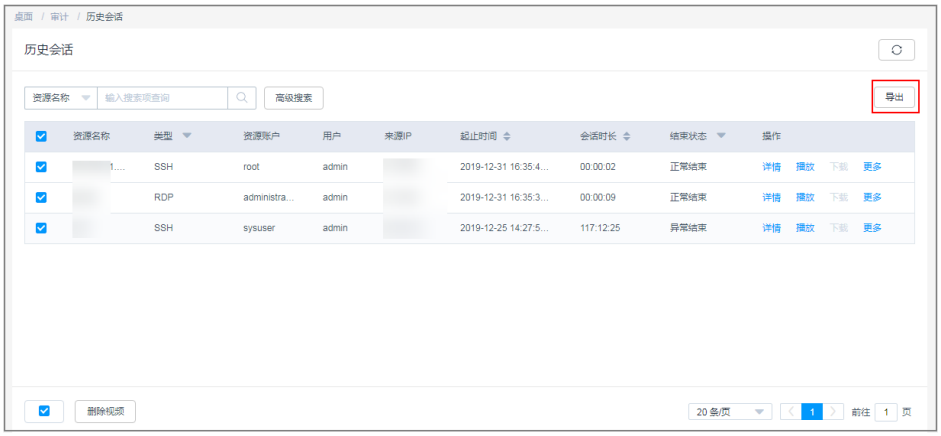
审计日志包括历史会话记录、会话视频、系统登录日志、系统操作日志、改密日志、账户同步日志等。

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 1-8 导出历史会话



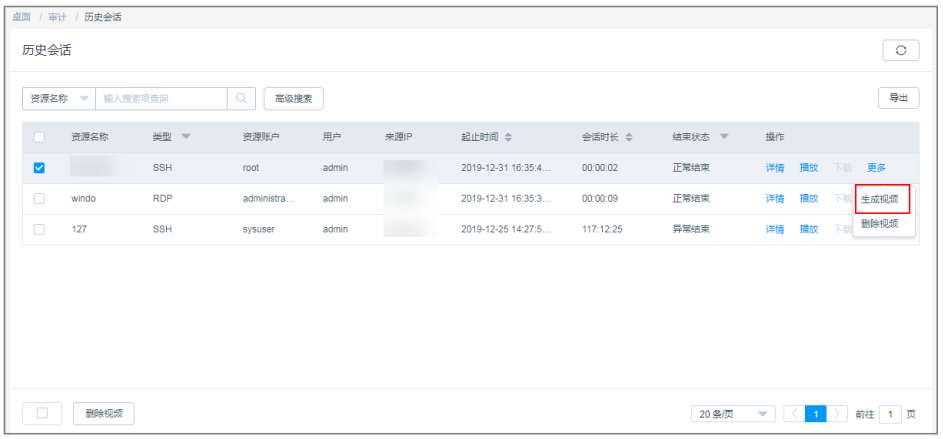
步骤3 下载会话视频。

说明

会话视频文件不支持批量生成和下载，需要逐个操作。

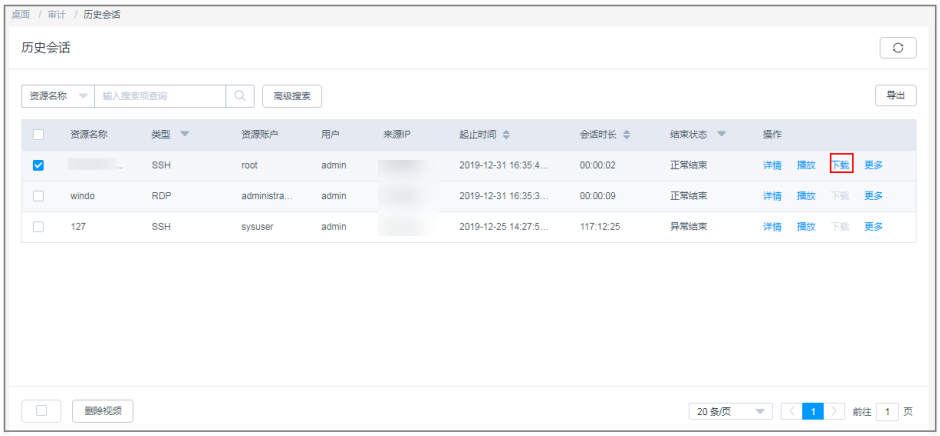
1. 选择“审计 > 历史会话”，进入历史会话页面。
2. 选择历史会话对应“操作”列“更多 > 生成视频”。

图 1-9 生成视频



3. 视频生成后，单击“下载”，将会话视频保存于本地。

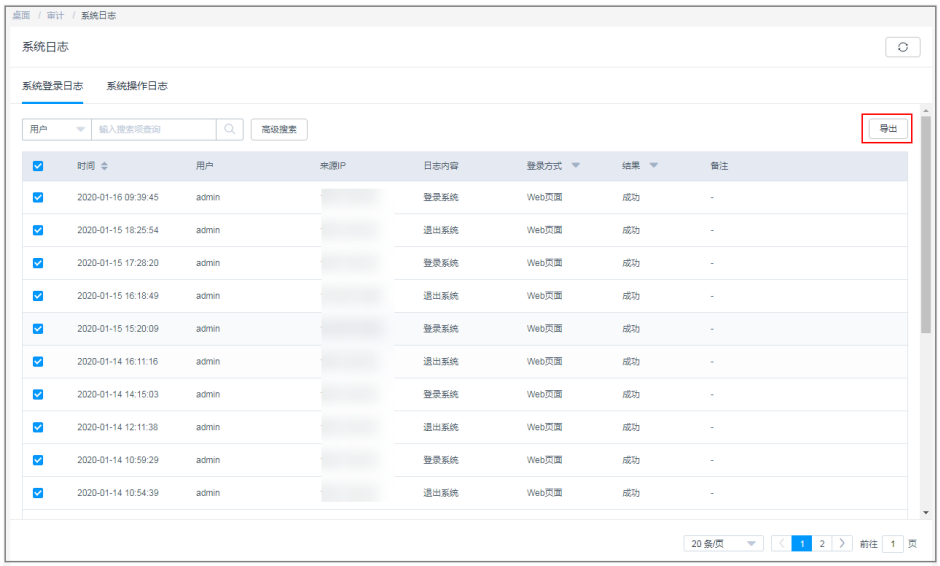
图 1-10 下载视频文件



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。

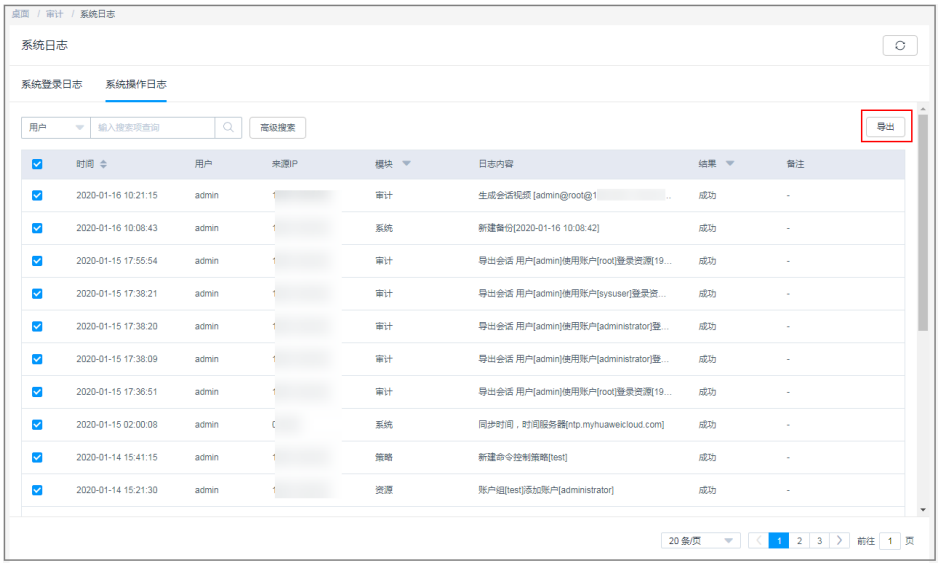
图 1-11 导出系统登录日志



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 1-12 导出系统操作日志



----结束

1.3 变更版本规格

前提条件

- 已获取管理控制台的登录帐号与密码。
- 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1-13**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 1-13 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

1.4 变更规格后验证

1.4.1 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 1-14 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 1-15 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。
   - 若一致，则变更规格成功。
   - 若不一致，需联系技术支持。

----结束

1.4.2 （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 1-16 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。若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 1-17 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 1-18 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

1.4.3 （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。

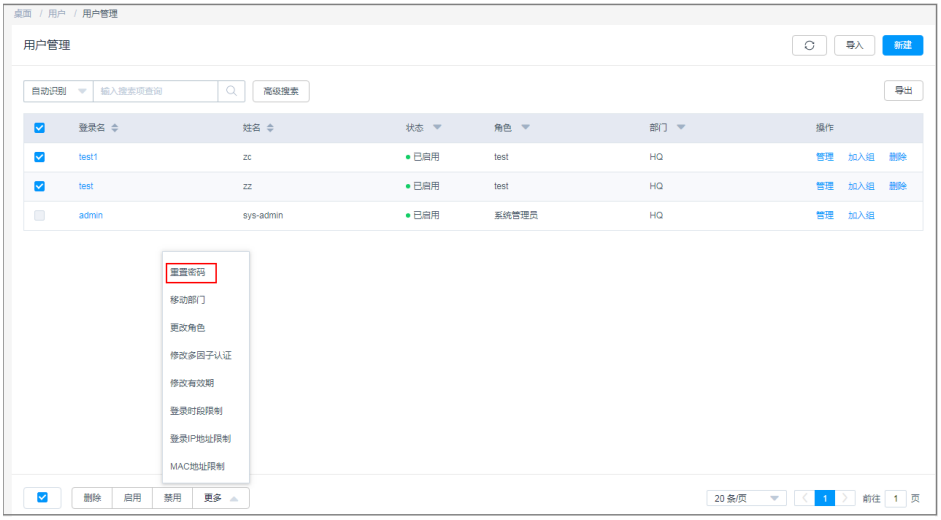
步骤2 选择“用户 > 用户管理”，进入用户列表页面。

- 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 1-19 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 1-20 批量重置密码

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。若不选择，则默认导出全部用户。

图 1-21 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 1-22 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 1-23 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 1-24 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

1.4.4 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1-2。

表 1-2 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。

2 数据库运维高危操作的复核审批

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。

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

- 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。
- 运维用户**User_A**已获取资源**RDS_A**的访问控制权限。

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。

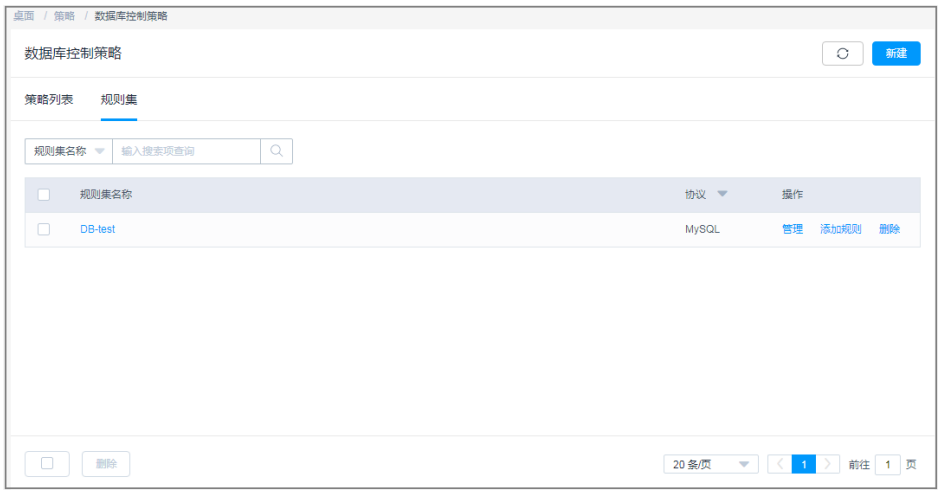
步骤1 **admin_A**登录云堡垒机系统。

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 2-1 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。

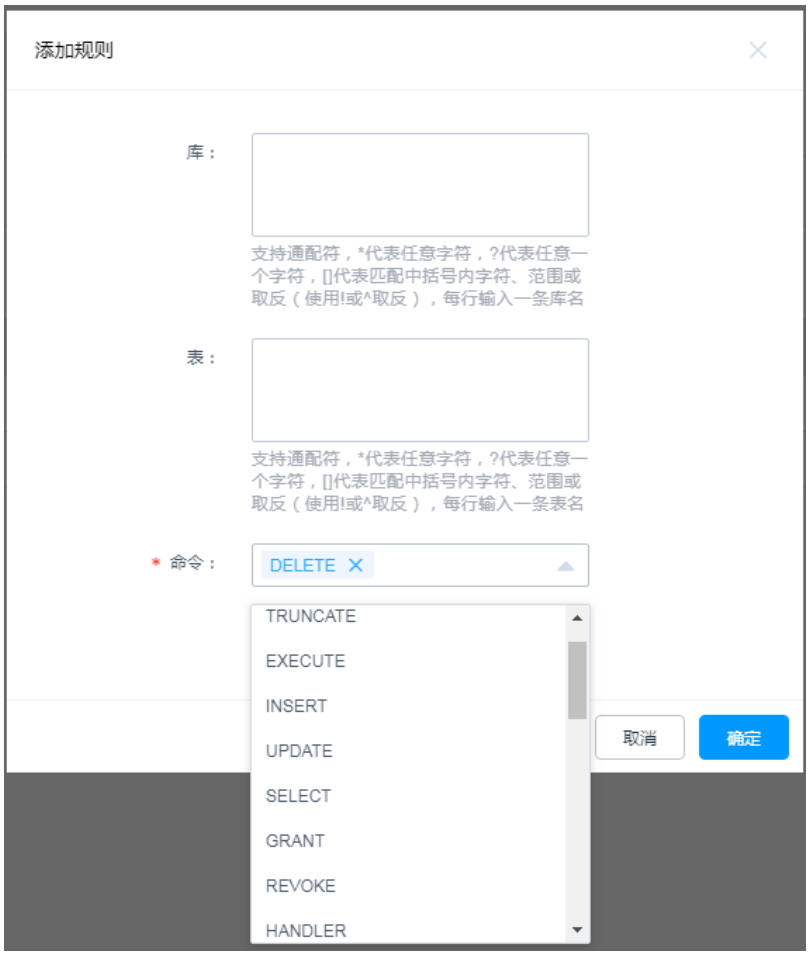
图 2-2 创建规则集

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 2-3 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 2-4 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 2-5 配置动态授权

3. 关联规则集**DB-test**。

图 2-6 关联规则集

4. 关联用户**User_A**和关联资源**RDS_A**。

图 2-7 关联用户和资源

----结束

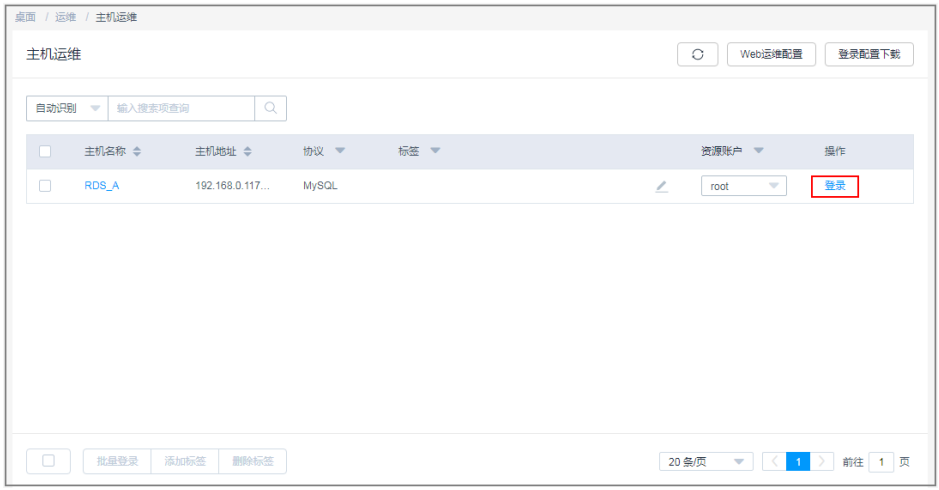
效果验证

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**。

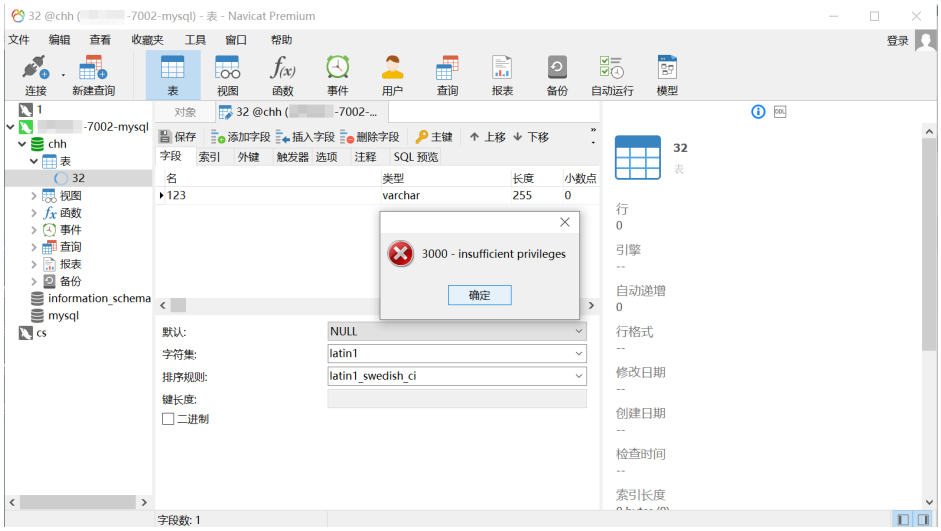
1. 登录云堡垒机系统。
2. 选择“运维 > 主机运维”。
3. 单击“登录”，通过SSO单点登录工具调用数据库客户端，登录数据库资源**RDS_A**。

图 2-8 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 2-9 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 2-10 提交数据库授权工单

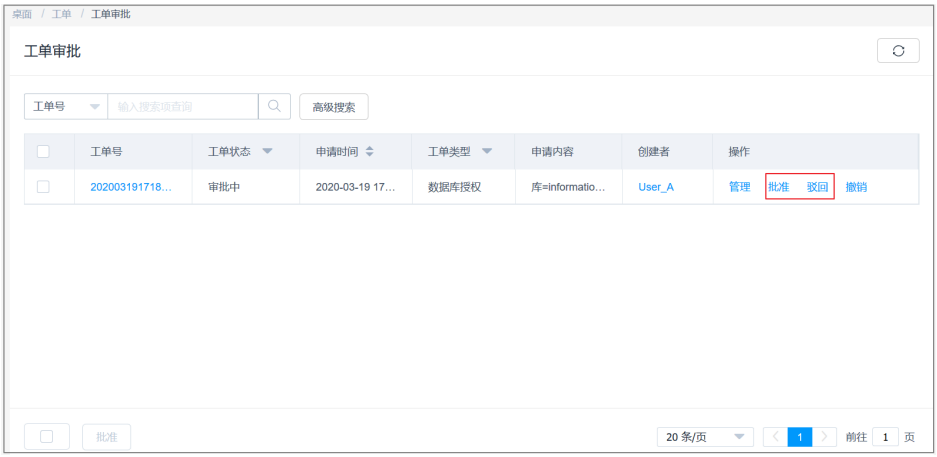
步骤4 管理员**admin_A**审核运维用户**User_A**的运维操作，根据实际情况批准或驳回申请。

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 2-11 审批工单



----结束

A 修订记录

发布日期	修订记录
2022-12-01	第一次正式发布

