保密级别: □绝密 □机密 □秘密 □内部公开 ■公开

# 旗舰版堡垒机-UHAS 用户手册



优刻得科技股份有限公司

	入口回门心水											
版本编号 或者更改 记录编号	*变化 状态	简要说明(变 更内容和变更 范围)	目期	変更人	审核日期	审核人						
V1.0	А	旗舰版堡垒机 3.4.8.0 版本	2021.4.11	薛姣	2020.4.21	安全产 品部						
*变化状态:		加. M——修改.		*	*							

文档修订记录

# 目 录

1前言	5
1.1 名称解释 1.2 适用范围和先决条件	
1.3 文持信息	
2产品间介	6
2.1 产品概要 2.2 应用场景	
3桌面	7
4部门	8
5 用户	8
5.1 用户管理 5.1.1 用户配置	
5.1.2 批量配直 5.1.3 田户导λ	9
5.2 用户组	
5.3 角色	
5.4 多因子 USB KEY	14
5.5 多因子动态令牌	
5.6 多因子手机令牌	
5.7 手机短信登求	17
6资源	18
6.1 主机管理	
6.1.1 新建主机	18
6.1.2 主机导出/导入	19
6.2 应用发布	
6.2.1 应用服务器	20
6.2.2 应用导出公司	21
0.2.3 应用导出/导入	
0.5 页	
0.4 贩户组	
7 年度	
(	25
7.1 访问控制策略	
7.1.1 访问控制策略	25
7.1.2 访问控制策略双人授权	26

7.2 命令控制策略	
7.2.1 命令控制策略	27
7.2.2 命令集	
7.3 数据库控制策略	
7.3.1 数据库控制策略	
7.3.2 规则集	
7.4 改密策略	
7.4.1 改密策略	
7.4.2 改密日志	
7.5 账户同步策略	
7.5.1 账户同步策略	
7.5.2 执行日志	
7.6 配置备份策略	
7.6.1 配置备份策略	
7.6.2 执行日志	
8 运维	36
8.1 主机运维	
8.1.1 登录配置卜载	
8.1.2 页面批量登录	
8.1.3 H5 登录字符协议主机	
8.1.4 H5 登录图形协议主机	
8.1.5 SSH客户端登录	40
8.1.6 SFTP/FTP 客户端登录	41
8.1.7 数据库客户端登录	
8.1.8 MSTSC 登录	
8.1.9 Web 运维配置	
8.2 应用运维	
8.3 脚本管埋	
8.4 快速运维	
8.5 运维仕务	
9审计	
91	50
92 历中会话	50
93 系统日志	51
9.5 示死百心 9.4 沄维报表	52
95系统报表	53
96 报表自动发送	53
10 上毕	54
10.1 访问授权工单	54

10.2 命令授权工单	56
10.3 数据库授权工单	
10.4 工单审批	
11 系统	58
11.1 安全配置	
11.1.1 用户锁定配置	
11.1.2 密码策略配置	
11.1.3 web 登录配置	
11.1.4 web 证书配置	
11.1.5 客户端登录配置	61
11.1.6 USB Key 配置	
11.1.7 手机令牌配置	
11.2 网络配置	
11.2.1 网络接口列表	
11.2.2 DNS 配置	
11.2.3 默认网关	64
11.2.4 静态路由配置	
11.2.5 OpenVPN 配置	
11.3 HA 配置	
11.4 端口配置	
11.5 外发配置	
11.5.1 邮件配置	
11.5.2 短信配置	
11.5.3 SNMP Agent 配置	
11.6 认证配置	
11.6.1 AD 域认证配置	
11.6.2 RADIUS 认证配置	
11.6.3 LDAP 认证配置	70
11.6.4 CAS 配置	71
11.7 工单配置	
11.7.1 基本模式	
11.7.2 高级模式	
11.7.3 审批流程	
11.8 告警配置	74
11.8.1 告警方式配置	
11.8.2 告警等级配置	
11.9 审计配置	
11.10 系统风格	
11.11 数据维护-存储配置	76
11.11.1 存储概览	

11.11.2 网盘空间	77
11.11.3 自动删除	77
11.11.4 手动删除	78
11.12 数据维护-日志备份	
11.12.1 本地备份	78
11.12.2 远程备份至 syslog 服务器	79
11.12.3 远程备份至 FTP/SFTP 服务器	
11.13 系统维护-系统状态	
11.14 系统维护-系统管理	
11.15 系统维护-配置备份与还原	
11.15.1 备份列表	
11.15.2 配置还原	
11.16 系统维护-授权许可	
11.17 系统维护-网络诊断	
11.18 系统维护-系统诊断	
11.19 关于系统	85
12 附录	86
12.1 应用发布服务安装配置	
12.1.1 安装 RemoteApp 跳板程序	86
12.1.2 配置 FireFox	
12.1.3 配置 Chrome	

## 1 前言

#### 1.1 名称解释

角色名称	主要权限
部门管理员	本部门的系统管理员,拥有管理权限。
策略管理员	策略管理员,拥有配置策略的权限。
审计管理员	拥有查阅、管理系统审计数据的权限。
运维员	拥有对资源的运维操作权限。

注:预置系统管理员 admin 不属于以上任何角色,拥有最高权限。

## 1.2 适用范围和先决条件

优刻得旨在为 IT 审计员、IT 顾问和安全专家提供可靠的服务器和应用发布管理安全解决 方案,帮助 IT 决策者应对各类法令法规(如 SOX、PCI、企业内控管理、等级保护、 ISO/IEC27001 等),同时帮助 IT 运维人员更高效地执行自动化运维和资源监控操作。本手册 编写以帮助用户了解系统使用、根据使用场景构建出属于自己的云计算安全管控系统。

要成为一个合格的堡垒机系统管理员,必须具备以下技能:

- 基本的系统管理 (Windows、Linux、Unix 以及各类网络设备) 知识
- 熟悉计算机网络、TCP/IP 协议以及常用网络术语

## 1.3 支持信息

优刻得科技股份有限公司

网址: <u>http://www.yunanbao.com.cn</u>

技术支持: 4000188133

## 2 产品简介

#### 2.1产品概要

堡垒机是优刻得科技股份有限公司经过多年研发,用于提供云计算安全管控的系统和组件,实现对运维资源的 4A 全面安全管控。系统包含用户管理、资源管理、策略、审计、工单等模块,支持对 Windows 主机、Linux 主机等诸多主机的安全管控保护。是集统一资产管理与单点登录,多种终端访问协议,文件传输功能于一体的运维安全管理与审计产品,产品特色及优势主要体现以下几个方面:

无需客户端,在登录资源,或对其实时监控和上传下载文件时无需安装任何客户端软件。 集中账号管理,统一维护主机、网络设备和应用发布等资源。

记录与审计,支持访问历史记录回放和操作指令搜索功能,可随时查看每个用户对所属主机、主机和网络设备的访问情况。

细粒度的权限划分及对用户的动态授权功能。

敏感命令拦截,对堡垒机所管控的主机进行实时命令拦截。

协同运维功能,可邀请其他运维人员或专家对同一会话进行协同操作或问题定位。

堡垒机系统为政府部门、电信运营商、金融机构、企事业单位、商业组织等提供了完整的 统一安全管理平台解决方案,使客户在面对高复杂度的内控授权、运维操作审计、法律法规合 规性审查时,能够实施完善的解决方案。

部署堡垒机,能够极大的保护客户内部网络设备及主机资源的安全性,提高运维效率,使 得客户的网络管理更加统一、安全和便捷。

#### 2.2应用场景

**满足政策、法规需求**: 堡垒机能满足各类法令法规(如 SOX、PCI、企业内控管理、等级 保护、ISO/IEC27001 等)对运维审计的要求。能够细粒度地划分不同角色的权限,达到控制管 理员对服务器的访问,并且提供大数据智能审计功能,对所有运维操作能达到很好的审计、监 控、控制和历史回放效果。

**管理外部 IT 运维人员**: 许多公司聘请了外部 IT 运维人员来进行各类主机和设备的配置、维护和管理,这些主机中可能包含着重要的邮件、客户信息和关键业务服务,这种行为实

际上意味着公司需要绝对信任外部 IT 运维人员。在这种情况下,拥有可靠的外部设备来监控、审计运维操作就显得至关重要。部署堡垒机后,既能满足对 IT 运维人员所有操作的记录和回放,又能实时监控与阻断在线 IT 运维人员,达到对外部 IT 运维人员操作的全监控。

**会话协同**:通过分享 URL,邀请其他用户共同查看同一会话,并且参与者在会话发起者批准的前提下可对会话进行操作,可应用于远程演示、对运维疑难问题"会诊"等场景。

远程管理的控制: 许多公司都拥有需要在互联网上远程管理的主机和设备, 部署堡垒机, 更好的强化对主机或设备的安全管理, 追踪每次运维操作的具体细节。

SSH、TELNET、RDP、VNC、SFTP、FTP 协议控制: 堡垒机能对 SSH、TELNET 等字符 控制协议提供支持,利用自身技术优势,无论对加密协议 (如 SSH、RDP、SFTP) 或非加密协议 (如 TELNET、VNC、FTP) 都能实现完全的监控和事后审计。让用户对支持不同协议的设备监控和审计操作更加简单和易用。

应用中心: 堡垒机的应用托管功能,可以实现 RemoteApp 应用程序的托管,同其他协议 一样,可以对其进行完全的实时监控、历史回放和审计功能。使用应用托管,将可以进行更 多,更大范围的运维审计,如 MySQL 数据库、浏览器等多种应用程序。

#### 3 桌面

E1 00	cuoua							<u>↓</u> ∃	Qadmin 👻
	桌面	_	14 用户	11 主机	<b>1</b> 应用	1 应用服务器		0 告鉴	
	部门用户	~	⊥ 活动用户	3	待审批工单	2	主机类型统计		
•	资源	~	admin sys-admin	183.238.16.138 2021-04-23 11:26:57	<b>admin</b> sys–admin	201910221719577909524 访问授权工单			
9	策略	~	admin sys-admin	183.238.16.138 20201230 11:01:52	admin sys-admin	201910221719579502878 访问授权工单	0	SSH	SFTP
щ.	运维	~	admin sys-admin	183.238.16.138 2020–12–30 11:01:44			$\mathbf{O}$	TELNET	i VNC
Ë	审计	~						FTP	
	工单	č							
×	赤机		😨 应用类型统计		▲ 当前活动会话		上 今日新增会话		
			0			0 会话数	0 会话数	0B 会话大·	dv.
				Chrome	字符	o	字符		0/0B
					图形	0	图形		0/08
					文件传输	0	文件传输		0/08

桌面由不同的控制板组成,控制版的数据来源于对应权限的模块,当有相应控制板权限时则显示对应的控制板内容。Admin 拥有最高权限。如图 3-1

图 3-1

## 4 部门

部门用于划分组织结构,可在每个部门下创建多个部门,以树状图结构展示出。如图 4-1 注意事项:

- 1 主机资源或者用户被添加到任何一个新建的部门后,此时删除该部门,该部门中的用户
   和资源会一并删除。
- 2 总部为默认部门无法删除。
- 3 当设置部门的安全码之后,部门的管理员在进行导出资源、用户等数据时,会自动使用 部门安全码进行加密

							<u> </u>	Q Q	admin 👻
Ŧ	桌面		· 桌面 / 館门						
đ			部门					0	新建
-	用户	~	部门名称 学 输入探索项量询 〇.						
۲	资源	~	1867	安全码	用户数	主机数	操作		
9	策略	~		00	14	11	新建下级	重命名	
w	运维	~	□ ▼ 总部1	00	2	2	新建下级	重命名	删除
Ű	审计	~		00	2	0	新建下级	重命名	删除
	I#	~		00	0	0	新建下级	重命名	删除
⊘	系統	~	別試組	00	3	1	新建下级	重命名	删除
		Ξ	☐ 2360/53页 #88						

图 4-1

## 5 用户

## 5.1 用户管理

## 5.1.1 用户配置

在用户管理页面可为堡垒机添加用户并分配角色,创建完成后点击用户后方的管理,可为 该用户配置多因子登录方式,用户的有效期,登录的时间段限制,登录时的 IP 地址限制, Mac 地址限制。如图 5-1

当用户开启多因子登录时,该用户不可使用密码登录方式登录,支持开启多个多因子方式 登录。

CI 00						🛓 🗐 🗘 admin 📼
-		桌面 / 用户 / 用户	编辑用户配置		×	
đ		admin	<b>8</b> 田子认证:	□ 手机锁接 □ 手机会牌 □ 115RKay □ 动态会绪		
<u>.</u>		****	PRIME.	- THE THE COOL ADDRESS		
		ť	有效期:	生效时间		
		<u>91</u>	登录时段限制:	允许登录 禁止登录		
	角色	修		周一 周二 周三		
		用户配置		周日 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23		∠编辑 ≪
۲			The THE STATE AND AND A			
۲			豆 <b>來</b> P地址成制-	煮名₽		
ŵ		•				
Ĩ				每行输入一个IP地址或地址阅,支持子网掩码,例如: 182.168.1.10-192.168.1.100或192.168.1.10/24		
B	工单	登录时。	登录MAC地址限制:	黑名单		
•				取消	确定	
			周五周六周六月			

图 5-1

#### 5.1.2 批量配置

堡垒机支持批量配置用户,勾选需要配置的用户后,点击更多,可批量更改。可支持批和 单个禁用用户。用户为禁用状态时,该用户无法登陆堡垒机。如图 5-2

								⊥ 🗐 💭 admin 🛩
-	桌面	桌面 / 月	8户 / 用户管理					
Ψ	部门	用户管	理					0 \\(\bar{\bar{\$\ber{\bar{\$\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bar{\br}}\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bar{\bre{\bar{\bar{\bar{\bre{\bre{\bre{\bre{\bar{\bar{\bar{\bre{\bre{\bre{\bre{\ber{\ber{\ber{\bre{\bre
•	用户	自动识	3月 ▼ 輸入授業項重询	<ol> <li>高级搜索</li> </ol>				导出
	用户管理		登录名 ⇔	姓名 ⇔	状态 👻	角色 👻	部门 🗸	操作
	用户组		James	james	<ul> <li>已启用</li> </ul>	部门管理员	总部	管理 加入组 删除
	角色		cui	崔磊	<ul> <li>已启用</li> </ul>	部门管理员	总部	管理 加入組 删除
	USBKey		lucas	soloution	<ul> <li>已启用</li> </ul>	test	总部	管理 加入组 删除
	动态令牌		test123	12	<ul> <li>已启用</li> </ul>	這推员	总部	管理 加入组 删除
•	27.10	100	op03	維運人員01	• 已启用	运维员	测试组	管理 加入组 删除
	英源		op02	維運 重置密码	<ul> <li>已启用</li> </ul>	运维员	测试组	管理 加入组 删除
9	策略		op01	維運 移动部门	<ul> <li>已启用</li> </ul>	运维员	测试组	管理 加入组 删除
m	运维		test001	test(更改角色	<ul> <li>已启用</li> </ul>	all	总部	管理 加入组 删除
Ŭ	审计		123	123 修改多因子认证	<ul> <li>已启用</li> </ul>	all	总部	管理 加入组 删除
	工单	. 🖬 )	bmgly	部门修改有效期	<ul> <li>已启用</li> </ul>	部门管理员	总部	管理 加入组 删除
	医统		ceshi	登录时段限制 cesh	<ul> <li>已启用</li> </ul>	运维员	部门A	管理 加入组 删除
	11:20		test	登录IP地址限制 test MAC地址限制	• 已启用	all	御部	管理 加入组 删除
		<b>2</b> 8	.选13/14项 删除	启用 禁用 更多 🔺			共 14 条 20	条/页 👻 🤇 1 🗦 前往 1 页

图 5-2

## 5.1.3 用户导入

支持用户导入,导出用户模板后按照模板格式添加用户可成功导入,目前导入用户的格式 支持 xls, xlsx, csv 格式文件。如图 5-3

E.U	cloua		(4					土 🗐 💭 admin 💌
			产 / 用庁管理	导入用户				
m		用户管	理	11 12 18 16 .	2+728			○         等入         新建
<u></u>				下戰機做: 黑田下戰				
		目初识		上传文件:	点击上传			
			登录名 💠		只能上传xls/xisx/csv文件		部门 👻	操作
			James	更多选项:	覆盖已有用户		总部	管理 加入组 删除
							.es	管理 加入组 删除
			lucas			取消 确定	<b>彩</b> 部	管理 加入组 删除
				12	• 已启用	這维员	总部	管理 加入组 删除
				總運人員01	<ul> <li>已启用</li> </ul>	透维员	测试组	管理 加入组 删除
				艏運人員02	• 已启用	這维员	测试组	聲理 加入組 删除
0				撤運人員01	<ul> <li>已启用</li> </ul>	這難员	测试组	管理 加入组 副除
ци Ш				test001	<ul> <li>已启用</li> </ul>	all	总部	智理 加入组 删除
Ű				123	<ul> <li>已启用</li> </ul>	all	总部	管理 加入组 删除
B				部门管理员	• <b>巳</b> 启用	部门管理员	85	管理 加入组 删除
-				ceshi	<ul> <li>已息用</li> </ul>	這難员	部门A	管理 加入组 删除
~				test	• 已启用	all	关部	管理 加入组 删除
		-						
		28	进13/14项 删除	启用 预用 更多			共 14 亲 20 条/页	👻 < 👖 🤇 期往 🧵 页

## 5.2 用户组

用户组用于把用户分组后,实现批量授权的功能,可创建多个组,点击编辑组成员可为该 组添加用户。如图 5-4

									<u> </u>	I Q	admin 👻
-	桌面		桌面 / 用户	桌面 / 甩戶 / 甩戶組							
ψ	部门		用户组							0	新建
1	用户	^	用户组名	5級 💌 输入搜索项查询							
	用户管理			用户组 ⇔			部门 🔻	成员数	操作		
	用户组			组2			总部	4	管理 编辑组成员	删除	
	角色			値1			总部	4	管理 编辑组成5	删除	
	USBKey										
	动态令牌										
۲	资源	~									
•	策略	~									
	运维	~									
Ë	审计	~									
B	工単	~									
-	系统	~									

## 5.3 角色

进入用户-角色模块,可查看到当前拥有的所有角色,堡垒机默认角色为 4 个,部门 管理员,审计管理员,策略管理员和运维员,角色拥有不同的权限,可新建自定义角色,并可 随意分配给该角色权限。如图 5-5

								<u>+</u> 🔳	🔉 admin 📼
		東西 / 用户 / 角	新建角色				~		
		角色	配置新建角色的权限						) Mit
		0020		新行建治部门	修改部门	删除部门			
	用户管理	AN ES-EMP	(二) 部门	修改安全码A	清除安全码A	查看安全码A			
		<b>A</b> E		修改安全码B	清除安全码B	查看安全码B		銀竹	
		III 1873	○ 用户	新建用户	修改用户	删除用户		管理	恢复默认
		m ma						管理	恢复默认
		100 W3+	USBKey	签发USBKey	吊销USBKey			管理	恢复激化
		(T) 1010	③ 动态令牌	签发动态令牌	吊销动态令牌			新理	恢复默认
		(T) all						10.10	mitte
			○ 主机管理	新建主机	修改主机	删除主机			
		test.					_	1873	MINE
		test-	○ 应用服务器	新建应用服务器	像改应用服务器	删除应用服务器		管理	明な
m		test-						管理	部院
B	工单					щxл IIIII	MI XE		
-	系统								
							共8条 20条/页 "		前往 1 页

图 5-5

#### 【角色控制范围】

新建角色的时候可以根据实际情况自行设置角色管理者,即如下图所示:

	gili		62 ( 30	88	新建角色	×	_
zîs			角色				0 12
*		^	8688	· MARKERIN Q.	• #8:	新聞2144个公司在学校,先行输入文 学、学校、自学校**	
				Ab	<b>供用</b> (2)	0 He O Hill	n.
				107885		#26月8月3月6日9日1日7月1日11日日 #26月8月3月6日9日1日7月1日11日日 理念部目开关,则是不知己和管理者:否则	與民國自治管
					《蓝角色甘浸有:		A REPA
				NUMBER .		月前村, 6为色世理素如果说此为色的用户, 成本将其电用户 修改为此为色	T. INSPAC
				241			S DEBI
				and the second s	• ND524	BARARETER BERAREN, BARENERBERRA	5 89
٠		Ť			-	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
0		× 1			象色描述	Mail on the American	
÷		~					
10		~				m21mm120+23中23中23中2	
в		~				RH <b>T-#</b>	
0		~					
		=	Ba	452 800		用5条 23条件 平 【 1	MG 1 2

角色管理者支持多选,且下拉备选项的显示范围即"功能权限开启新建用户或修改用 户权限的角色"。

若已开启了设置角色管理者,角色详情页面显示设置角色管理者为开启状态,并显示 角色管理者,如下图:

	桌柄		道西 / 用户 / 角色 / 角色洋橋			
ŵ	<b>a</b> X()		测试员			
	用户		【基本信息		∠ 編編	η.
	用户管理					
	用户组		用他, 制武改			
			管理的原: 开闢			
	LISRKey		《金페色憲法書: 圖用			
	-		角色世理者; 新门管理员, 则武员			
			用他搬送: -			
•	678		1 million		1.000	
•	50.05		用他的限			· ^ ·
	运输		標記	2008	50 K	
Ű.	#it		应用态地		1619	
	I#		3.5L5H		638	
۰	系统		访问授权工单	新建访问授权工单、传改访问授权工单、删除访问授权工单	1819	
		Ξ				_

图 5-7

若未开启了设置角色管理者,角色详情页面显示角色管理者为禁用状态,且不显示角

	皇王		点面 / 用户 / 向色 / 角色评情											
ф	<b>#</b> ()		策略管理员											
	用户	~	基本信息		∠ 編編 ▲									
to and														
	HI TELE		角色: 頒幣管理员											
	用户组		教授6項: 开启											
			②重命色哲理者: 第用	心默动色的变化 熱雨										
	USBKey		角色振送: 策略管理员,拥有数量策略权限											
	动态令牌													
•	資源	~	角色胶顶		∠ 編編 ∧									
		~												
•	1000	Ť	(E12)	708	80									
	运输	~	<b>部</b> (1)	律改安全码B、语阶安全码B、重整安全码B	1979									
Ŭ.	审计	~	用户		819									
в	I#	~	主机管理		819									
	NE44	~	应用服务器		819									
			应用发布		<b>昭時</b>									
			资源财产		1929									
			访问控制策略	新建访问控制策略。得改访问控制策略、删除访问控制策略	1928									
			命令没利策略	新建命令控制策略、修改命令控制策略、戦争命令控制策略	839									
			改電頻時	新建改市策略、特改改市策略、影响改市策略、市药加油收入	639									
			数据库控制预用	新建設媒体控制領導。學改設媒体控制領導。影映設媒体控制領導	819									
		÷												

图 5-8

【注】

色管理者,如下图:

- 如果不开启角色管理者,则表示不限制角色管理者,那么当用户创建(或修改)用户时, 可以设置(或修改)用户为该角色;
- 如果开启角色管理者,则表示仅角色为角色管理者的用户(在用户有"新建用户"功能权限的情况下)能够创建该角色的用户,或者是(在用户有"修改用户"功能权限的情况下)将其他用户修改为该角色。

## 5.4 多因子 USB key

当用户配置好可用多因子 USBkey 登录时,可在 USBkey 模块中中为该用户签发 USBksy,插入 USBkey 后,选择需要签发的用户和正确 PIN 码,签发成功后,被签发的用户 可正常使用 USBkey 方式登录堡垒机。如图 5-9、图 5-10

	<i>ड</i> ीती)	ALL F. M. F. MARKE	USB Key配置							
di.		系统配置								
		安全配置 网络配置 HA配置	USBKey :	龙脉科技	-		U15			
+		國家方式配置		2018年4日交 北京CA					2.988	
				海察方面	取2時	4802				
100		取以登録方式: 密码登录, 学	0(÷#	吉大正元						
Ш.		LUSB Kevőlitt							< 1000	
в		1 and royana								
•		USB Key: 22384482								
		根证书列表						C 数向认证	十添加	
		#714 SEX13	50.20 <del>m</del>		KOMALINE ©		WT51M 0	18/12		
					智无数据					

图 5-9

5**-**11

	435	成型 化用产 / USBKey	签发USBKey		×			
<sub>th</sub>		USBKey						O EX
=		USexey - solvestes Q ROSE	<ul> <li>USBKey:</li> </ul>	请施入USBKey 🐨				
		USERRY C	• 無顧用户:	诸法将关款用户 · · ·		医发射器 牛	题作	
			• PINH:	诸幅入PIN码				
					ROM ROZ			
+								
ø								
-								
8								
в								
۰								
		C Edward						

图 5-10

吉大正元 USBKey 签发登录需要选择证书,证书必须与关联用户一直才能登录成功。如图

			*-4001220101000		_		
		gt.BL / Hith / USBKey	签发USBKey		×		
		USBKey	• 关联用户: fest1	-			OB
	-	USBKey - MARSON					
		USBKiry \$	证书框		<b>10:0</b>	接作	
			名称 本发表 内図測试ー Private Certif	过期日期 [证书类型]			
			1. 2700 BK	and a laware (and )			
				_			
	~			用 頭定 取消			
	~						
	~						
	~						
	~						
	÷						
		CI EUBO/OXE Aires					

图 5-11

# 5.5 多因子动态令牌

当用户配置好可使用多因子动态令牌登录时,可在动态令牌中为该用户签发动态令牌。点 击签发后输入标识和正确的秘钥并选择要关联的用户,点击确定,被签发的用户登录堡垒机时 可使用多因子动态令牌方式登录。且动态令牌支持导出导入的方式添加保存。如图 5-12

ΞU	ctoup						⊥ 🗐 🗘 admin ∞
		桌面 / 用户 / 动态令牌	签发令牌标识		×		
đ		动态令牌	<ul> <li>今席标识:</li> </ul>				○ 号入 新業
		令牌标识 - 输入搜索示查询		长度为1-128个汉字或字符			导出
		② 令牌标识 \$	* 秘钥:			鉴发时间 ≑	操作
		2100000436905	* 关联用户:	请选择关联用户		2021-04-09 11:15:20	吊精
					_		
					取消 确定		
۲							
0							
m							
Ë							
B							
۲							
		已 已迭0/1項 用 44				共1条 20条/页 👻	1 页

图 5-12

# 5.6 多因子手机令牌

手机令牌登录做为登录堡垒机的登录方式之一,用户可在个人中心-手机令牌中按照步骤 绑定,绑定成功后可使用手机令牌登录方式登录堡垒机中。如图 5-13

E U			$\pm$	admin 🔺
-	桌面		桌面 / 个人中心	♀ 个人中心 □ 退出
đ	部门		个人中心	
•	用户		个人中心 手机令牌 我的权限 我的日志	
	用户管理		绑定手机令牌	8
	用户组			
	角色			
	USBKey			
	动态令牌			
۲	资源			
9	策略		手机令牌已绑定,点击"解除"可解除绑定。	
	运维		9782	
Ë	审计		_	
Ē	I¥			
	系统			
		≡		

# 5.7 手机短信登录

在创建用户时为用户添加手机号码(该号码用户登录堡垒机之后可在个人中心自己设置) 或者点击已创建的用户后方的管理为用户添加手机号码,并在登录配置中配置可以使用多因子 手机短信即可。如图 5-14

<b>E</b> U							⊥ 🗏 💭 admin 💌
-			桌面 / 用户 / 用户管理 / <b>用</b> 户	编辑用户基本信息		×	
æ			test	2127.96 10.	-		
		^	基本信息	• Kuter.	本地		∠ 编辑 《
				* 姓名:	test		
	用户组		登录名: 1	test	长度为1-255个汉字或字符,允许输入汉 字、字母、数字、"@"、"."、"_"或"-"		
	白色		认证类型: :	本地 手机:		7	
			姓名:	test	手机号十分重要,请输入正确的手机号码		
			手机: *	邮箱:			
			邮箱:	14** * 角色:	all		
	资源	Ť	角色:	all * 所属部门:	日本		
۲	策略	Ý	所屬部门:	总部	104 Mb		
Ψ		~	身份证号:	身份证号:			
Ë		~	用户描述:	- 用户描述:			
Bì	工单	~	创建者:	adm			
		~	创建时间:	2019		取消 确定	
			修改者:	admin			
		≡	修改时间:	2020-01-15 10:06:38			

第17页共89页

6 资源

#### 6.1 主机管理

#### 6.1.1 新建主机

进入资源-主机管理,可展示当前所被堡垒机管控的所有主机,点击新建后可添加新的资源主机。如图 6-1

C U								<u>↓</u>	📃 💭 admin 🔻
			主机管理	新建主机		×			
m		主机管理				1		0 自动发	砚 导入 新建
<u>.</u>		自动识别		* 主机名称:	长度为1-128个汉字或字符				鼻出
۲				* 协议类型:	MySQL			67/3	49.05
			nw ♀	<ul> <li>主机地址:</li> </ul>	SSH			「「「「」、	freferer 更多
			ucas_test_k 15		RDP			测试组	管理 更多
			<sup>~</sup> 州-UDB 10	* 端口:	VNC			总部	管理 更多
			数据库审计 10		FTP			総部	管理 更多
			Windows测试 10	系统类型:	SCP			总部	管理 更多
۲			inux-vnc iC vindows测试机 10	编码:	请选择编码	]		48.2	管理 更多
щ.			sftp-Linux 10	更多选项:	✓ 文件管理 ✓ X11转发			总部	管理 更多
Ú			_inux-内网 10		🗹 上行剪切板 🛛 🔽 下行剪切板			总部1	管理 更多
Bì			Windows-内 10	* 所属部门:	部			总部1	管理 更多
-			自建数据库 10			取消下一步		总部	管理 更多
	_	□ 已选0/1	1项 删除	添加标签 删除标签	更多 💌		¥	11条 20条/页 💌 <	1 〉前往 1 页

图 6-1

新建主机资源时涉及主机地址为 IPv6 以及 IPv4 主机地址协议为 MySQL, DB2, Oracle, SQL Server 时不支持账户的验证, 即隐藏验证按钮, 如下图 6-2, 图 6-3:

111 U	CLOUD								<u>+</u>	🔄 🔲 🔍 admin 🤻
			桌面 / 资	源 / 主机管理	新建主机		×			
ф			主机管	理	* 士机之政:				〇 自动发	現 导入 新建
*		~	自动识	<b>列 👻</b> 输入搜索项查询		长度为1-128个汉字或字符				导出
۲		^		名称 💠 📑	* 协议类型:	MySQL	- 1		部门 🗸	操作
				ssh-key主机 1	* 主机地址:		- 1		总部	管理 更多
				lucas_test_k 1	5	请输入有效的IP地址或域名	- 1		测试组	管理 更多
				广州-UDB 1	0 * 端口:	3306 语输入1_65535之间的方效数字	- 1		总部	管理 更多
				数据库审计 1		M4874-00002-01818 AXX-7-	- 1		总部	管理 更多
				Windows测试 1	系统类型:	请选择系统类型	- 1		总部	管理 更多
۲		~		linux-vnc 1	) 编码:	请选择编码	- 1		总部	管理 更多
				windows测试机 1			- 1		总部	管理 更多
άū		~		sftp-Linux 1	更多选项:	✓ 文件管理 ✓ X11转发	- 1		总部	管理 更多
Ē		~		Linux-内网 1		✓ 上行剪切版 ✓ 下行剪切板	- 1		总部1	管理 更多
Bì		~		Windows-内 1	* 所属部门:	总部	- 1		总部1	管理 更多
									总部	管理 更多

图 6-2

() () ()	CLOUD													1	Ξ	Q admin
					/ 主机管理	新建主机						×				
ŵ			3	主机管理			添加账户:	○ 立即添け	10 〇 以后添加					〇自动发	R 5	み 新建
*		~		自动识别		绚	NTROM KIND	•								导出
۲		^			夕政 ▲		登录方式:	自动登录		•			- 118		提作	
					ssh-key主机	10	主机账户:		÷				总部		管理更	3
					lucas_test_k	15		? <u>\</u> 74X.9%				_	测试组		管理 更	3
					广州-UDB	10	* 密码:						总部		管理 更	3
					数据库审计	10	账户描述:						总部		管理 更	\$
					Windows测试	10							总部		管理 更	\$
-						10		描述最长1	28个汉字或字符			- 1	总部		管理 更	\$
ø		Ť			windows测试机	10						_	总部		管理 更	3
m		~				10				取消	上一步 發	定	总部		管理 更	\$
Ŭ		~			Linux-内网	10.13.48.217	22	\$	SSH				总部1		管理 更	\$
B		~			Windows-内	10.13.73.92	3389	F	RDP				总部1		管理 更	3
		~			自建数据库	106.75.179.170	3306	1	MySQL	Linux			总部		管理 更	\$
, v																

图 6-3

## 6.1.2 主机导出/导入

堡垒机支持批量导出/导入用户,可点击导出后按照导出的模板规范填写参数,正确填写后可批量导入主机,目前支持导入的文件格式有 xsl/xlsx/csv。当进行导出的主机所在部门有安全

密码时,则在本地打开的时候需要输入正确的加密密码。勾选验证账户时,则可在任务中心查 看主机账户正常/异常数。导入界面如图 6-4

🖾 U					-						L 🗐 💭 admin 🤝
				原 / 主机管理	导入主机				×		
m			主机管理	里		导入方式。		= ) 二十約		〇 自动2	親 导入 新雄
			自动识别	<ul> <li>輸入搜索项查:</li> </ul>	Ð	470120	▼ MXIT47 ∪	4/AIN			<b>9</b> 出
۲						下载模板:	点击下载				
				名称 🗢	*	上传文件:	点击上传			部[] -	
				lunge test k	15		只能上传xls/xlsx/cs	v文件		测试组	管理 史罗
	资源账户			广州-UDB	10	更多选项:	覆盖已有主机	验证账户		总部	管理 更多
				数据库审计	10				mo4 Text	总部	管理 更多
				Windows测试	10.13.73.92	23	TELNET	Windows	AC/1	总部	管理 更多
	系统类型				10.13.48.217	5901	VNC	Linux		总部	管理 更多
	tale m/s	~									

图 6-4

堡垒机支持云主机导入,选择云平台后,输入正确的 public\_key 和 private\_key 后,当点击全 部导入时则导入全部主机到堡垒机,点击让我选择时可手动选择要导入的主机,导入后可在主 机管理中查看该主机。如图 6-5

						_	4	🖞 🗐 🤤 aomin 🗸
			原 / 主机管理	导入主机		×		
		主机管理	里	导入方式:	○ 从文件导入    □ 导入云主机		〇自动发	現导入新建
	~	自动识别	■ 輸入援索項査询	<ul> <li>云平台:</li> </ul>				导出
	^		名称 💠 📑		腾讯云 AWS Azure		郭门 →	操作
			ssh-key主机 1		O UCloud		总部	管理 更多
			lucas_test_k 1	<pre>s * public_key:</pre>	0		测试组	管理 更多
			广州-UDB 1	* private_key:			总部	管理 更多
			数据库审计 1				总部	管理 更多
			Windows测试 1	project_id:	0		总部	管理 更多
•	$\sim$		linux-vnc 1	0 优先导入IP:	○ 公网 ○ 内网		总部	管理 更多
m	$\sim$		windows测试机 1	) 更多选项:	覆盖已有主机		总部 	管理 更多
			sftp-Linux 1				88	管理 史多
Ħ	Ť			PT/ALEN J.	98.65		8 m	
	Ý			标签:			8 m	等理 面名
	~				取消 让我选择 刍	全部导入	2010	64.2.2

图 6-5

## 6.2 应用发布

#### 6.2.1 应用服务器

创建应用发布之前,需要为该应用创建应用发布服务器,需要输入正确的服务器地址,选择服务器类型,当服务器类型选择完成后,程序启动路径会自动填写。如图 6-6

3 U								🛓 🗐 🗘 admin 💌
			源 / 应用发布	新建应用服务器		×		
æ		应用发行	布	<ul> <li>- 昭久昭夕初·</li> </ul>				○ 与入 新建
*		应用列表	远用服务器	- 100 ET 110 C 2001 -	长度为1-128个汉字或字符			
۲		自动识别	1 ▼ 输入搜索项查询	• 服务器地址:				导出
			服务器名称 ♠		请骊入有效的IP地址或域名		1.	操作
			chrome浏览器	* 类型:	请选择协议类型		8	管理 删除
				* 端口:	请输入1-65535之间的有效数字			
				• IR& # P - :				
				· 1,00,868 (C,300) -				
۲				* 密码:				
m				* 所属部门:	总部			
Ú				* 程序启动路径:				
Ē								
•						取消 确定		

图 6-6

## 6.2.2 应用

应用发布服务器创建完成后,可创建应用并且关联应用服务器,输入正确的应用地址和端 口后点击下一步添加账户即可。如图 6-7

						<u> </u>	I U admin ™	
-		樂面 / 资源 / 应用发布	新建应用	×				
'n		应用发布	* 应用名称:			0	导入 新建	
*		应用列表 应用服务器		长度为1128个汉字或字符				
۲		自动识别 👻 输入搜索项查询	* 应用服务器:	请选择应用服务器			导出	
		应用名称 ◆ 应用	* 所属部门:	「「「」」を書いていていていていていていていていていていていていていていていていていていて	账户数	部门一	操作	
		chrome -			 2	总部	管理 更多	
			应用地址:	请输入有效IP或域名				
			应用端口:					
				请输入1-65535之间的有效数字				
۲			应用参数:	数据库类应用请输入数据库名				
			更多洗项:	文件管理  上行剪切板  下行剪切板				
Ü								
Bì			文件保存:	🗌 保存上传文件 🔛 保存下载文件				
•				取消下一步				

图 6-7

#### 6.2.3 应用导出/导入

支持应用发布服务器和应用导出/导入,可导出模板后按照模板格式填写正确参数后导入, 导入应用时,前提需要有对应的应用发布服务器,否则无法直接导入应用。目前支持的导入文 件格式有 xls/xlsx/csv。当进行导出的用户所在部门设置了安全码时,则在本地打开的时候需要 输入正确的部门安全码。如图 6-8

[]] U								土 🗐 🗘 admin 🔻
-			/ 应用发布	导入应用服务器		×		
ŵ		应用发布		下载模板:	点击下载			○ 号入 新建
		应用列表	应用服务器	上传文件:	点击上传			
۲		自动识别	★ 输入搜索项音询		只能上传xls/xlsx/csv文件			导出
				更多选项:	3 覆盖已有应用服务器			
			服务器名称 💠				1~	操作 19104
			chrometa, p. es			取消 确定	2)	<b>查注 開</b> 体
۲								
Ψ								
Ú								
B								

图 6-8

#### 6.3 资源账户

每创建一个主机或应用后, 主机中会自带一个空账户【Empty】, 该账户用于手动登录。 除此之外, 可为主机创建多个账户, 点击新建, 选择关联的资源主机和登录方式后输入正确账 户密码即可。当添加和配置好正确的 sshkey 时, 可直接使用 sshkey 免密码登录。支持批量删 除可批量验证所选择的账户正常/异常状态。如图 6-9

III U	CLOUD								⊥ I Q	admin 🤝
			图源 / <b>资源账户</b>	新建账户		×				
æ		资源则	行	* 关联资源:	请选择关联资源 💌				О <b></b> \	新建
*		资源则	3.2 ★ 補入搜索項查询	登录方式:	0283					鲁田
۲			资源账户 ⇒ 1	1	日初豆家		;方式 📼	部门 💌	操作	
			[Empty] #	* 资源账户:			)登录	总部	管理 加入组	删除
			[Empty] #		特权账户		]登录	总部1	管理 加入组	删除
			[Empty] #	* 密码:			)登录	总部1	管理 加入组	删除
			[Empty] #	SSH Key:		ן	)登录	总部	管理 加入组	删除
			[Empty] #				)登录	总部	管理 加入组	删除
			[Empty] #		填写之后将优先通过SSH Key登录	J	]登录	总部	管理 加入组	删除
			[Empty] #	passphrase;			]登录	总部	管理 加入组	删除
Ψ.			[Empty] #	¢			)登录	总部	管理 加入组	删除
Ú			[Empty] #	切换自:	请选择资源账户 🔻		)登录	测试组	管理 加入组	删除
Bì			[Empty] #		请选择从哪个账户切换为该账户		)登录	总部	管理 加入组	删除
_			root #	inteas.			)登录	总部	管理 加入组	删除
Ň	234.026		root			取消 确定	)登录	总部1	管理 加入组	删除

图 6-9

注:

登录方式可选择自动登录,手动登录,提权登录。当选择提权登录时,需要选择提权到那 个账户,提权时的切换命令,最后输入正确密码即可。

特权账户用户改密策略改密,勾选特权账户时,该账户属于特权账户。

账户导出/导入与应用导入操作相同。

若资源账户关联的主机资源涉及主机地址为 IPv6 以及 IPv4 主机地址协议为 MySQL,

DB2, Oracle, SQL Server 时不支持账户的验证,即隐藏验证按钮,如下图 6-10:



图 6-10

## 6.4 账户组

账户组可将账户打包分组,实现批量授权的功能,可创建多个账户组,创建完成后可为该 组增加/删除账户,支持批量删除组和批量验证账户组中账户正常/异常的状态。如图 6-11

() []]							_				<u>↓</u> [	Q Q	admin 💌
Ŧ			8源 / <b>账户组</b>	新建账户组			×						
ф		账户组	1	* 账户组:		united and the March & March						0	新建
	~	账户组	1名称 ▼ 输入搜索项查询		长度为1-64个汉子 字母、数字或"-"	或子付,允许输入汉子、							
۲	^		账户组 ⇔	账户组描述:			_	操作					
			H组		描述最长128个汉言	『或字符	_	管理	添加成员	移除成员	#UR		
			C组				_	管理	添加成员	移除成员	删除		
			B组				取消 确定	管理	添加成员	移除成员	删除		
			A					管理	添加成员	移除成员	删除		
						总部	0	管理	添加成员	移除成员	删除		
ø	~												
Ψ	~												
É	~												
Bì	~												
۲	~												

图 6-11

### 6.5 系统类型

进入资源-系统类型,可查看到堡垒机内置系统类型,点击新建后可创建新的系统类型,

如	존	6-	12
玔	ž	6-	12

							_	⊥ 🗏 IQL admin 👻
				1週 / 系统类型	新建系统类型		×	
			系统类	型	<ul> <li>系統类型:</li> </ul>			O 新建
		~	系统类	撃 - 論入總索項查询		长度为1-128个汉字或字符		
		^			改密参数:	命令     成功返回    十	Ū	
	主机管理			系统类型 🗢		使用{password}表示旧密码, {new_pass word}表示新密码, {change_user}表示需		
				Linux		要以密的资源账户, 个文持的手付()		
				Windows	提权账户改密参数:	هو         لي المركز المم	Ū	
				Cisco		使用{password}表示旧密码, {new_pass word}表示新密码, 不支持的字符()		
	账户组			Huawei				
				НЗС	配置备份参数:	命令    成功返回    十	Ū	
				DPtech		使用{backup_file}表示备份文件别名, {ip} 表示备份服务器IP地址, {port}表示FTP端 口 {username}表示FTP账户条 {nassw		
		~		Ruijie		ord}表示FTP登录密码,不支持的字符()		
		~		Sugon	描述:			
		~		Digital China sm-s-g10-		取消	肖一确定	
Bì		~		Digital China sm-d-d10-	-000			
-		~		ZTE				
				ZTE5950-52tm				

图 6-12

说明:

参数为非必填,每个参数最多添加5个。

改密参数:设置改密的命令和成功返回。

提权账户改密参数:设置提权账户改密的命令和成功返回。

配置备份参数:设置配置备份的命令和成功返回。

#### 7 策略

#### 7.1 访问控制策略

#### 7.1.1 访问控制策略

访问控制策略用于控制用户访问资源的权限,可以让指定的用户在指定的时间内访问指定 的主机资源。且支持 IP 地址限制,文件传输,剪切板上下行,水印显示等。选择完成后关联 用户和资源,所关联的用户就能使用关联的资源进行运维。如图 7-1

(1) U									$\downarrow$		Q. admin 🤝
-				/ 访问	新建访问控制策略						
æ			访问控制题	<b>휷略</b>	<ul> <li>         等于 1000000000000000000000000000000000000</li></ul>					0	新建
*		~	策略名称	- 3	And and the later	长度1-64个汉字或字符,允许输入英文字母、数字、或"-"					鲁田
۲		×		策略名	* 部门:	总部	操作				
۲		^		himore	有效期:	生效时间 ① 失效时间 ③	管理	关联	更多	删除	
					文件传输:	✓ 上传 ✓ 下载					
				test-g	面底进顶:	▼ 文体整理 ● 上行能机械 ● 下行能切断 □ 易示水印	管理		更多	删除	
				策略所	至少远坝· 春憂时段限制:		管理	关联	更多	删除	
				admin	and the second of		管理		更多	删除	
						a    ]   3  2					
	配置备份策略			级从高		周五 周六 周日					
ιώα.		ř				0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23					
Ü		ř			IP限制:	黑名单 👻					
Bì		×				取消 下一步					
•		ř									

图 7-1

当账户存在于多个策略时,并且策略中选择的功能不同,可通过拖动策略,更改优先级。支持 策略启用/禁用功能。如图 7-2

🖾 υςιουρ							<u> </u>	Ξ (	) admin 🔻
- ■ 桌面	桌面 / 策略	/ 访问控制策略							
<b>止</b> 部门	访问控制	〕策略						0	新建
▲ 用户 ~	策略名称	▼ 输入搜索项查询	٩	高级搜索					导出
参 资源 ~		策略名称	状态 💌	用户	账户	操作			
✓ 策略 へ		himore-test-pol1	<ul> <li>待完善</li> </ul>	≛ admin	X -	管理 关联	更多	删除	
访问控制策略									
命令控制策略		test-gaojing	<ul> <li>待完善</li> </ul>	± 123 m -	± - m -	管理 关联	更多	删除	
数据库控制策略		策略所属部门	<ul> <li>已禁用</li> </ul>	L ceshi	± =	管理 关联	更多	删除	
改密策略				击 组1	- h C组				
账户同步策略		admin	<ul> <li>已启用</li> </ul>	≞ admin; test m =	<sup>三</sup> administrator@数据库审计-跳板机-Wi 品 -	管理 关联	更多	删除	
配置备份策略	列表按照优	先级从高到低排序,支持	笔动改变优先级顺序						
型 运维 ン									
■ 审计 ~									
∎ I¥ ✓									

图 7-2

## 7.1.2 访问控制策略双人授权

添加双人授权候选人后,当策略内的用户访问策略内的资源时,需要候选人现场输入密码。可在访问控制模块点击策略后的更多选项添加双人授权候选人。如图 7-3

	桌面		桌面 / 策略	1 / 访问控制策略					
.m.	部门		访问控制	间策略				O	新建
·	用户	~	策略名称	▲ 輸入搜索项查询	Q	高级搜索			导出
۲	資源	~		策略名称	状态 🔻	用户	账户	操作	
٢	策略	^		test2	<ul> <li>已过期</li> </ul>		≝ accsec@res sec	管理关联更多删除	
				test		T admine co	acceeders sec. administrator@ft	管理 羊联 面名 删除	
	命令控制策略			1651		m -	т		
	数据库控制策制	M.	列表按照优	优先级从高到低排序,支持	推动改变优先级顺序			双人授权候选人 (0)	]
	改密策略								
	账户同步策略								
	配置备份策略								
Ŧ	运维	~							
Ü	审计	~							
<b>_</b>	工单	~							
\$	系统	~							

图 7-3

## 7.2 命令控制策略

#### 7.2.1 命令控制策略

命令控制策略用于控制指定的用户登录指定的字符类型协议后,当执行策略指定的命令 时,会触发相应的执行动作限制,执行动作分为:允许执行,拒绝执行,断开连接(断开运维 会话),动态授权(生成工单申请授权)。可配置该策略有效期,不在有效期内时,策略状态 为未生效。如图 7-4

(1) [1]	CLOUD			⊥ 🗉 Q admin 🔻
-		桌面 / 策略 / 命令 新建策略	×	
đ		命令控制策略	之前:	0 新建
-		策略列表 命令	长度1-64个汉字或字符,允许输入英文字母、数字、或""	
۲		策略名称	部门: 总部	
۲		□ 策略名称 * 5	<b>动作:</b> 请选择执行动作 **	操作
		- 动态拦截	<b>2次期:</b> 生效时间 ①	管理 插入 关联 删除
		test拦截		管理插入关联剧除
		列表按照优先级从高	100- 同二 周二	
			周四 周五 周六 周日	
m			取消 下一步	
Ĥ				
B				
-				
		□ 已选0/2项 删除	<u>鳥用 禁用 共2条 20条/页 ▼</u>	(1)前往1页

图 7-4

配置完成后添加命令或命令集,添加命令支持通配符,最后关联用户和资源即可。如图

7-5

(1) U									⊥ 🗐 🗘 admin 👻
-				⑧略 / 命令控制策略	新建策略		$\times$		
æ			命令招	它制策略	关联命令 关联命令	ж.			⊖ 新建
<u>.</u>			策略列	表 命令集					
۲			策略之	· 输入搜索顶弯流	命令/参数:				
۲				10. 10. 0. 0. 0. 0. 0. 10 March 10		支持通配符,*代表任意字符,?代表任意		140	18.01
				动态拦截		或取反(使用!或^取反),每行输入一条命 令		жи <u>т</u> –	9#1F 管理 插入 关联 删除
				test拦截命令测试				▲ root@Linux-内网-測试机	管理插入关联 割餘
						取消	上一步		
m									
É									
Bì									
-	系统	~							

#### 7.2.2 命令集

命令集可添加堡垒机内置的一些命令,用于方便添加。可直接关联到命令控制 策略中。如图 7-6

(1) U									⊥ ⊑	ιų	admin 💌
Ŧ			桌面/策略/命	添加命令				<			
ħ			命令控制策略	命令/参数 🔻	输入搜索项查询	Q				0	新建
<b>±</b>		~	策略列表 命	命令		使用说明	命令描述				
۲		~	命令集名称 👻	. • .	inux主机						
۲		^	命令集	• •	文件管理				操作		
			<ul> <li>文件相</li> </ul>		cat	cat [-AbeEnstTuv] [help] [	把档案串连接后传到基本输出	ync; swapoff	管理	添加命令	删除
			123		chattr	chattr [-RV][-v<版本编号>][+/	. 这项指令可改变存放在ext2文件系统上的文件或目录.		管理		删除
	数据库控制策	é	測试		chgrp	chgrp [-cfhRv][help][versi	变更文件或目录的所属群组		管理		删除
					chmod	chmod [-cfRv][help][versi	变更文件或目录的权限				
	账户同步策略				chown	chown [-cfhRv][dereference	变更文件或目录的拥有者或所属群组				
					cksum	cksum [help][version][文件	检查文件的CRC是否正确				
	配置备份策略				cmp	cmp [clsv][-i <字符数目>][h	比较两个文件是否有差异				
m		~			diff	diff [-abBcdefHilnNpPqrstTuvw	比较文件的差异				
Ë		~			file	file [-beLvz〗-f <名称文件>〗	辨识文件类型				
Bì		~					取消 确定				
		~									

图 7-6

## 7.3 数据库控制策略

#### 7.3.1 数据库控制策略

数据库控制策略用于控制指定的用户登录到指定的数据库类型资源后执行的一些操作,当 登录数据库资源且执行策略中关联的规则时,会触发相应的执行动作限制,执行动作分为:允 许执行,拒绝执行,断开连接(断开运维会话),动态授权(生成工单授权)。可配置该策略 有效期,不在有效期内时,策略不会拦截。如图 7-7

目前数据库控制策略只支持 MySQL, Oracle 两种数据库。

121 U												<u>↓</u> 🗏	Д a	dmin 🔻
			桌面 / 策略 / 数据	新建数据库控制策略						$\times$				
ф			数据库控制策略										0	新建
		~	策略列表 规则	* 東船西柳	长度1-64个汉	字或字符,允许输入英文字f	母、数字、或""							
۲		~	· · · · · · · · · · · · · · · · · · ·	* 部门:	总部			•						
۲		^	96 89 47 76	执行动作:	断开连接			-				10.00		
			東暗古体 制除-限制									metr 管理 插入		HIX
				有效期:	生效时间	·	时间							
			列表按照优先级从高数	时间限制:	生效时段	失效时段								
					周二周三									
					周四周五周六									
					周日 0 1 2	345678910	11 12 13 14 15 16	17 18 19 2	0 21 22 23					
ŵ		~												
Ë		~							取消	下一步				
Bì		~												
♥		~												
					_		_		_	_		_	_	
	LOUD	i							-			<u>→</u> 🗏	Q a	dmin 💌
Ci UC	LOUD 桌面		桌面 / 策略 / 数据库控	制策略 新建规则	集				×			<u>↓</u> 🗏	Q a	dmin 💌
₩ UC 	<b>LOUD</b> 桌面 部门		桌面 / 策略 / 数編库控 数据库控制策略	新建规则	<b>集</b> 規則集名称:				×			<u>↓</u> ■	Q a	dmin マ 新建
	集面 部门 用户 〜		.4回 / 加級 / 数据库控制策略 数据库控制策略 策略列表 规则集	新建规则	<b>集</b> 规则集名称:		12.11.11.11.11.11.11.11.11.11.11.11.11.1		×			<u>↓</u> ■	Q a	dmin マ 新建
₩ UC 	<mark>火</mark> 面 東面 部门 用户 〜 资源 〜		<ul> <li>点面 / 預局 / 数据库控</li> <li>数据库控制策略</li> <li>策略列表 规则集</li> <li>规则集名称 ~ (a)</li> </ul>	新建规则 新建规则	<b>集</b> 规则集名称: 协议:	长度1-64个汉字或字符, 方 长度1-64个汉字或字符, 方 敬 文学、或*-**	论许输入英文字		×			<u>↓</u> II [	Q a	dmin >
	LOUD 桌面 部门 用户 〜 資源 〜 策略 へ	,	《三 / 第8 / 数据库控制策略 数据库控制策略 策略列表 规则集	制旗略 新建规则	<b>集</b> 规则集名称: 协议:	长度1-64个汉字或字符, グ 母、数字、或"-" MySQL MySQL	6许输入英文字		×		80 -	<u>↓</u> ] [	Q a	dmin -
₩ UC 	ACOUD 桌面 部门 用户 ~ 资源 ~ 策略 ~ 访问控制策略		<ul> <li>二回 / 加毛 / 数据库控制策略</li> <li>数据库控制策略</li> <li>策略列表 規則集</li> <li>規則集名称 - 和入</li> <li>規則集名称 - 和入</li> <li>規則集名称 - 和入</li> </ul>	28/2010年 - 19:10:00:00:00 - 19:10:00:00:00	<b>集</b> 规则集名称: 协议:	 长度1-64个汉字或字符, ƒ 母、数字、或"-" MySQL MySQL Oracle	论许输入英文字	取消	×		1812 -	▲ 目		imin >
₩ UC 	よい よの 単一 次面 部门 第四 次面 の 令 た 初期 第一 、 、 、 、 、 、 、 、 、 、 、 、 、		<ul> <li>《雨 / 角毛 / 数据属约</li> <li>数据库控制策略</li> <li>策略列表 规则集</li> <li>规则集名称 &lt; 他心</li> <li>规则集名称 &lt; 他心</li> <li>规则集名称 可用</li> <li>一 测试</li> </ul>	制旗略 新建规则	<b>集</b> 规则集名称: 协议:			取消	×		19 K ♥ MySQL MySQL	▲ 目	C S S S S S S S S S S S S S S S S S S S	fmin ~
₩ UC 	東面     部门       用户     、       預源     、       黄路     へ       访问控制策略     へ       会会控制策略        数据库控制策略		<ul> <li>第三 / 第三 / 数三萬</li> <li>数据库控制策略</li> <li>策略列表 規則集</li> <li>規則集名称 (加)</li> <li>規則集名称</li> <li>規則集名称</li> <li>規則集名称</li> <li>規則集名</li> <li>規則集名</li> <li>規則集名</li> </ul>	湖湖縣 新花建规则 建作为资源	<b>集</b> 规则集名称: 协议:	长度1-64个汉字或字符。 母、数字、或"" MySQL MySQL Oracle	6许输入英文字	取消	×		t∂iX ❤ MySQL MySQL	▲ 目	C ar	tmin マ 新建
₩ UC       	桌面           部门           用户           资源           次路           合令控制策略           会校制策略           数据库控制策略           改振路路		<ul> <li>二回 / 加毛 / 数据库控制策略</li> <li>数据库控制策略</li> <li>策略列表 規則集</li> <li>規則集名称 (私)</li> <li>規則集名称 (私)</li> <li>規則集名称 (私)</li> <li>規則集名称 (私)</li> <li>規則集名称 (私)</li> </ul>	(制) 第6章 纪 见 则	<b>集</b> 规则集名称: 协议:	[ 长度1-64个汉字或字符, ƒ 母、数字、或*-** MySQL MySQL Oracle	此许榆入英文字 ▲	取消	×		1812	▲ 目	Q a	dmin 💌
₩ UC 	点面         第           第         第           第         2           資源         4           方向控制策略         4           改振席控制策略         2           改振策略         5           改振策略         5		▲四 / 知母 / 数据库控 数据库控制策略 策略列表 規則集 規則集名称 < 個介 規則集名称 < 個介 □ 規則集名称 < 個介 □ 規則集名称 < 個介 □ 規則集名称 □ 規則集名称	(1) 新建规则 (1) 新建规则	<b>集</b> 规则集名称: 协议:	 长度1-54个汉字道字符, 5 年、数字、或"~"   MySQL   Oracle	t许输入英文字 《 ]	TER 3H	×		thi⊄ ❤ NySQL NySQL	→ 目	C C	Amin V
<ul> <li>□ UC</li> <li>■</li> <li>▲</li> <li>Ø</li> </ul>	桌面     部门       用户     >       預厚     >       資源     >       访问控制策略        会令控制策略        数据库控制策略        改密策略        医二合合分策略		(1) 第一 第二 大 数 (1) 大 3 (1) 大 3 (1) + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 +	(19) 第66 第71 建 規則	<b>集</b> 规则维名称: 协议:	长度1-64个汉字或字符, 分 母、数字、或"-" MySQL MySQL Oracle	6件输入英文字	R.M.	× Až		thit ~ Mysail Mysail	▲ 目		tmin -
<ul> <li>□ UC</li> <li>□</li> <li>↓</li> <li>◆</li> <li>♥</li> <li>♥</li> <li>♥</li> <li>♥</li> <li>♥</li> <li>♥</li> </ul>	桌面     #       第一     #       月户     //       资源     //       资源     //       资格     //       动向控制策略     //       改密策略     //       账户同步策略        配置备份策略     //       远继     //		<ul> <li>二回 / 加級 / 数据库控制策略</li> <li>数据库控制策略</li> <li>策略列表 規則集</li> <li>规則集名称 - 加ン</li> <li>规则集名称 - 加ン</li> <li>规则集名称 - 加ン</li> <li>规则集名称</li> <li>规则集名称</li> </ul>	(2) 新建設	<b>集</b> 规则集名称: 协议:	 长度1-04个汉字域字符, ƒ 甲、数字、域 <sup>*</sup> -* MySQL Oracle	1) 计输入英文字 	Run	×		th IX T	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		fmin w
<ul> <li>□</li> <li>□</li> <li>□</li> <li>●</li> <li>●</li></ul>	点面         部门           第二         次           資源         へ           資源         へ           方向控制策略         へ           改進库控制策略            改畫策略            設置条控制策略            設置条控制策略            設置条の策略            設置条の策略            認識            正            正            正            正            正            正		二回 / 知母 / 数据集約 数据库控制策略 策略列表 規則集 規則集名称 < 回入 規則集名称 < 回入 規則集名称 < 回入 規則集名称 < 回入	(2) 新聞紙 新建規則 (2) 小 (2) ) (2) 小 (2) ) (2) ) (	<b>集</b> 规则集名称: 协议:	长度1-54个汉字理字符, 5 母、数字、或"=" MySQL MySQL Oracle	:许输入英文字	R/H	× 49.72		1012 - MySQL MySQL	▲ 目		fmin ~
<ul> <li>□</li> <li>□</li> <li>↓</li> <li>◆</li> <li>♥</li> <li>■</li> <li>■</li></ul>	桌面        桌面        部门        周户        资源        资源        访问控制策略        改憲策略        設備库投制策略        改憲策略        配置各份策略        這進        审计        工单		(3)日 / 第時 / 数据展替 数据序控制策略 策略列表 規則集 規則集名称 - 第2 規則集名称 - 第2 規則集名称 - 第2 規則集名称 - 第3 規則集名称 - 第3 第3 第3 第3 第3	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	<b>集</b> 规则维名称: 协议:	 长度1-04个汉字或字符, ∮ 母、数字、或"-"   MySQL   MySQL Oracle	b许镇入英文字 	RCH	×		1012 V MySQL MySQL	<u>・</u> 第24 第24 第24 第24 第24 第24 第24 第24 第24 第24		imin w 新建

#### 7.3.2 规则集

规则集可添加堡垒机内置的一些 sql 命令,规则集创建完成后可为规则集添加规则,关联 到数据库控制策略中。如图 7-8

(1) U							土 🗐 🗘 admin 💌
		策略 / 数据库控制策略	添加规则		×		
ħ	数据	库控制策略	库:	user			C Mise
*	策略引	利表 规则集					
۲	规则	<b>集名称 ▼</b> 输入搜索项查询		支持通配符,*代表任意字符,?代表任意 一个字符,[]代表匹配中括号内字符、范围 或取反(使用!或^取反),每行输入一条库			
۲		規則集名称	w.	ă		协议 💌	操作
		删除不可用	ige -	w		MySQL	管理 添加规则 删除
		测试		支持通配符,*代表任意字符,?代表任意		MySQL	管理 添加规则 删除
		qw		一个字符,□代表匹配甲括号内字符、范围 或取反(使用!或^取反),每行输入一条表 名		MySQL	管理 添加规则 删除
			* 命令:	DELETE X			
				ALTER			
				TRUNCATE			
œ				INSERT	取消 确定		
-				UPDATE			
				SELECT			
Ê				GRANT			
-				DEVOVE			

图 7-8

#### 7.4 改密策略

#### 7.4.1 改密策略

改密策略用于对主机内资源账户定时,定期进行改密,改密方式可选择生成不同密码(多 个账户生成不同密码),生成相同密码(多个账户使用相同密码)和自定义相同密码(多个账 户指定密码),改密方式为生成不同密码和生成相同密码时,可以指定生成密码的策略,如图 7-9.当选择定时执行和周期执行时可在指定的时间自动执行改密策略;改密策略执行完毕 后,会将密码修改结果分开发给指定的用户,

(ii) U	CLOUD						⊥ 🗐 🗘 admin 💌
	桌面	桌面 / 策略 / 改密策略	新建策略		$\times$		
ŵ	部门	改密策略	* 销略实称:				O 新建
.≖	用户 ~	策略列表 改密日志	April PLA.	长度1-64个汉字或字符,允许输入英文字 母、 数字、或"-"			
۲	资源 🖌 🎽	<b>策略名称 ▼</b> 输入搜索项查询	* 部门:	总部			
۲	策略へ	□ 策略名称	* 执行方式:	请许择执行方式 👻		操作	
	访问控制策略					管理 立即执行 关联	删除
	命令控制策略		* 改密方式:	请选择改密方式			
	数据库控制策略	改密test	更多选项:	生成不同密码		管理 立即执行 关联	删除
	改密策略			生成相同密码 指定相同密码			
	账户同步策略		发送方式:	不发送			
	配置备份策略						
ŵ	运维 ~						
Û	审计 ~				取消下一步		
Ē	工单 ~						

注意:

1) 支持改密策略改密的协议有: SSH, MySQL, sql server, Oracle, RDP, Telnet.

2) 选中允许修改特权账户密码时,才能修改特权账户的密码,否则特权账户密码不会修

改, 默认不选中

3)选中使用特权账户改密时,系统自动寻找账户对应资源的特权账户,通过特权账户修改
 密码,无特权账户时,自己修改自己密码,该选项默认选中

4) 手动执行改密策略需要输入当前用户的登录密码

5)使用自定义改密策略时按照自定义改密策略创建密码;否则会生成 20 位的包含大小写 字母、数字、特殊符号的密码

#### 7.4.2 改密日志

改密策略执行完成后可在改密日志中查看改密详情。用户(具有下载改密日志权限)可通 过下载日志到本地查看改密策略改密之后的密码(其他用户只能查看大致信息,无法看到具体 的密码),下载与手动执行策略类似,需要输入操作用户的登录密码。如图 7-10

11 U	сголд								$\downarrow$		Q	admin 👻
Ŧ	桌面	桌面 / 策	略 / 改密策略									
ι. Έ	部门	改密策	路									0
Ŀ	用户 ~	策略列表	改密日志									
۲	资源 💙	策略名利	家 ▼ 輸入搜索項查询					全部	选择日期	范围		
٢	策略 へ		时间 🗢	策略名称	总数 🗢	成功 🗢	失敗 🗢	未修改 💠	操作			
	访问控制策略		2019-12-30 16:45:45	123	1	1	0	0	详情	下载	删除	
	命令控制策略		2019-12-27 16:27:01	123	1	1	0	0	详情	下载	删除	
	数据库控制策略		2019-12-27 16:24:04	123	1	1	0	0	详情	下载	删除	
	改密策略		2019-12-27 16:23:17	123	1	0	1	0	详情	下载	删除	
	账户同步策略		2019-12-27 16:07:51	123	1	0	1	0	详情	下载	删除	
	配置备份策略		2019-09-29 15:20:30	123	1	0	1	0	详情	下载	删除	
Ψ	运维 ~		2019-08-27 15:05:47	123	1	0	1	0	详情	下载	删除	
Ë	审计 ~		2019-07-12 16:11:47	改密test	1	1	0	0	详情	下载	删除	
Ĩ.	工单 ~		2019-07-12 15:58:23	改密test	1	1	0	0	详情	下载	删除	
\$	系统 ~		2019-07-12 15:57:04	改密test	1	1	0	0	详情	下载	删除	
		🗆 ex	先0/14项 删除				共 14	4条 20条/页		1 >	前往	1页

## 7.5 账户同步策略

#### 7.5.1 账户同步策略

账户同步用户拉取或推送账户,当选择拉取账户时,会扫描主机内的所有账户,统计正 常、非正常信息。选择推送账户时,将堡垒机录入的资源账户同步到目标主机,可进行更新主 机密码,新建主机密码,或删除非堡垒机纳管账户的操作。如图 7-11

[]] U	CLOUD						⊥ 🗐 💭 admin 🔻
		桌面 / 策略 / 账户同步策略	新建策略		×		
ŵ		账户同步策略	<ul> <li>* 策略名称;</li> </ul>				C 新建
*		策略列表 执行日志	200 B 10	长度164个汉字或字符,允许输入英文字 母、 数字、或""			
۲		策略名称 ▼ 输入搜索项查询	* 音序门:	总部			
۲		策略名称					操作
			* 执行方式:	手动执行			
			同步动作:	○ 拉取账户			管理 立即执行 天妖 劇隊
				扫描目标主机的所有账户,并统计所有正 常、 异常账户信息			
				● 推送账户 溶资源账户同步到目标主机。更新主机密			
				码、或新建主机账户、或删除主机非法账 户			
				🦳 账密不一致时,允许更新该账户密码			
	配置备份策略			账户不存在于主机,允许创建该账户			
m				主机存在非纳管账户,允许删除该账户			
畄			* 连接超时:	10 连接目标主机的招助财间 戰込值为10	]		
Bì				Addition and the second process of \$10(1) 100 and \$10(10) 20(10)			
•					取消下一步		
		□ 已选0/1项 删除	启用 禁用			共1条 20条/页	▼ 〈 1 〉 前往 1 页

注意:

1) 当选择同步动作为推送账户时,除选择执行账户时,还需要选择推送账户。

非纳管账户说明: 主机内的账户没有添加到堡垒机内, 该账户会被识别为非纳管
 账户。

3) 账户同步策略只支持 SSH 协议。

## 7.5.2 执行日志

账户同步策略执行后,可在执行日志中查看详情。如图 7-12

11 U	CLOUD						🛓 🗐 🎜 admin 👻
-	桌面	桌面 / 策略 / 账户同步策略					
ф	部门	账户同步策略					0
⊻	用户 ~	策略列表 执行日志					
۲	资源 ~	策略名称 ▼ 输入搜索项查询	٩			全部 选择	₽日期范围 <b>□</b>
۲	策略へ	□ 时间 令	策略名称	同步动作 🔻	主机执行概要	账户执行概要	操作
	访问控制策略	2021-04-23 15:31:08-2021	账户同步-测试	推送账户	•1 •0	更新密码: ● 0 ● 0	详情 下载 删除
	命令控制策略					新建账户: ● 0 ● 0 删除账户: ● 0 ● 0	
	数据库控制策略						
	改密策略						
	账户同步策略						
	配置备份策略						
ŵ	运维 ~						
Ë	审计 ~						
B	工单 ~						
<ul><li></li></ul>	系统 ~						
		□ 已选0/1项				共1条 20条/页 👻	〈 1 〉 前往 1 页

#### 7.6 配置备份策略

#### 7.6.1 配置备份策略

为了方便网络设备上配置文件的备份,堡垒机支持网络设备配置备份策略。创建时执行方 式可选择为手动执行,定时执行和周期执行,最后关联要执行的账户即可。执行完成后可在执 行账户所在主机下的配置备份中查看该文件(支持下载到本地)。且支持外置存储,使网络设 备能够备份到用户自定义的 FTP/TFTP 服务器上(对应的设备需要支持 FTP/TFTP 命令)。如 图 7-13
() () ()	CLOUD						🛓 🗐 🎜 admin 👻
			桌面 / 策略 / <b>配置备份策略</b>	新建策略		×	
ŵ			配置备份策略	* 節軟空动·			
*			策略列表 执行日志	. Yest 1199	长度1-64个汉字或字符,允许输入英文字 母、数字、或"-"		
۲			策略名称 ▼ 输入搜索项查询	* 部门:	总部		
۲			策略名称	* 执行方式:	Tabba -		操作
				- 34137334	L L M M M L		
				配置接收地址:			
					<b>审制人有效的PP地址</b>		
				存储方式:	TFTP 👻		
				外置存储:			
Ţ.					_	取消	
Ú							
Đ							
-							
		_	已选0/0项	启用 禁用			

图 7-13

## 7.6.2 执行日志

配置备份策略执行完成后,可在执行日志中查看详情,查看备份文件的的完成情况。如图

7-14												
	11 U	CLOUD									⊥ E <sup>0</sup>	🖉 admin 👻
	-	桌面		桌面 / 策略	/ 配置备份策略							
	ф.	部门		配置备份	)策略							0
	•	用户	~	策略列表	执行日志							
	۲	资源	~	策略名称	▼ 輸入搜索項查询 Q.					全部	选择日期范围	ä
	0	策略	^		时间 💠	策略名称	总数 💠	成功 💠	失敗 🗇	操作		
		访问控制策略			2021-04-23 15:37:38	策略备份	0	0	0	详情 下载	删除	
		命令控制策略										
		数据库控制策略	8									
		改密策略										
		账户同步策略										
		配置备份策略										
	₩	运维	~									
	Ĩ	审计	~									
	Bì	工单	~									
	ື	系统	~									
			Ξ	已送	0/1項 删除				共1条	20 条/页	▼ < 1 >	前往 1 页

图 7-14

## 8 运维

#### 8.1 主机运维

#### 8.1.1 登录配置下载

进入[运维/主机运维],点击<登录配置下载>,可将运维资源导出成 xshell 或者是 secure CRT 配置,如图 8-1。详细操作流程可查看登录配置下载文件中的 readme.txt 文件。

(1) U										🛓 🗐 💭 admin 👻
-			维 / 主机运维	登录配置下载						
æ		主机运	维	登录配置下载	SecureCRT	XShell			C Webi	四维配合 登录配置下载
-		自动识别	<b>列 🗢</b> 输入搜索项查询	文件名编码:						
۲			主机名称 ⇔						资源账户 🔻	操作
۲			自建数据库			I	以消 确定	Z	root 💌	登录
m			数据库审计跳板	106.75.156.92:3389	RDP				adminis 💌	登录
			广州-UDB	10.13.157.111:3306	MySQL				root 💌	登录
			windows测试机	10.13.73.92:21	FTP				adminis 💌	登录
	脚本管理		Windows测试内网	10.13.73.92:23	TELNET				adminis 💌	登录
			Windows-内网-测	10.13.73.92:3389	RDP				adminis 💌	登录
			sftp-Linux-内网	10.13.48.217:22	SFTP				root 💌	登录
			Linux-内网-测试机	10.13.48.217:22	SSH				root 💌	登录
Ü				10.13.48.217:5901	VNC				root	登录
B										
•										
			<b>先0/9項</b> 批量3					#	9条 20条/页 👻	

图 8-1

#### 8.1.2 页面批量登录

进入[运维/主机运维],点击<登录>,会登录主机资源进入 H5 会话,且支持批量登录,勾需 要登录的主机,点击下方的<批量登录>,便可登录成功。当没有勾选主机时,批量登录为灰 色,不可点击。如图 8-2。

C U	CLOUD									↓ 🗐 💭 admin 🗸
Ŧ	桌面		桌面 / 运	维 / 主机运维						
.m	部门		主机运	维					C Webiz	维配置 登录配置下载
•	用户	~	自动识	别 ▼ 输入搜索项查询						
۲	资源	~		主机名称 ⇔	主机地址 ⇔	协议	标签 👻		资源账户 🔻	操作
0	策略	~		自建数据库	106.75.179.170:3306	MySQL		Z	root 💌	登录
ŵ	运维	^		数据库审计跳板	106.75.156.92:3389	RDP			adminis 🔻	登录
				广州-UDB	10.13.157.111:3306	MySQL		··· _	root 🔍	登录
	应用运维			windows则就机 1、选择批量	<b>登陆资源</b>	FTP		📃	adminis 🔻	登录
	脚本管理			Windows测试——内网	10.13.73.92:23	TELNET		🖉	adminis 💌	登录
	45/22/24			Windows-内网-测	10.13.73.92:3389	RDP		··· _	adminis 💌	登录
	快速运班			sftp-Linux-内网	10.13.48.217:22	SFTP		🖉	root 📼	登录
	运维任务			Linux-内网-测试机	10.13.48.217:22	SSH		··· <u>/</u>	root 📼	登录
Ë	审计	~		linux-vnc	10.13.48.217:5901	VNC		··· _	root 🔍	登录
E	工单	~								
	系统	~								
					0 占土业	=×/±+穴灯				
				382/0175 SH-B-S	人、 只 古 机 ·	里豆饨按钮		+	0.6 00.50	
		Ē		Walawi TITE	2.0K 0010032 000	0.00.02		9 9	сож 20 ж/Щ ▼	▲ 1 页

图 8-2

注意

不支持批量登录的协议有: FTP/SFTP/SCP/DB2/MYSQL/Oracle/SQL Server, 手动登录和 双人授权账户。

#### 8.1.3 H5 登录字符协议主机

进入[运维/主机运维], 登录 SSH 或 TELNET 协议主机进入 h5 会话页面, 根据所拥有权限 可执行相应操作, (如: 管理员如没有给予运维员下载权限, 则在 H5 页面下载按钮不可使 用) 如图 8-3。

图 8-3

说明:

1.可上传本地文件和网盘文件。

2.可将该主机内文件下载到本地可网盘。

3.网盘属于堡垒机用户的个人空间,仅本人可见,用户可以将网盘文件上传到多个主机。

4.如果主机开启了文件保存,运维时与主机进行了文件传输,符合要求的文件在审计中能保留下载

SSH 或 TELNET 协议主机 h5 会话的登录,支持协同分享。如图 8-4,创建者可以将当前会话的链接复制,发送给堡垒机用户。



图 8-4

堡垒机用户可通过该链接登录创建者的会话中,如图 8-5。

an an transmission and a second a		
	会活协同邀请 如外科电片,用自留记录号于审计。 3.8 aa 的能时间 2018-07-23 17:48:13	
	立即进入	
	OTO-1-TON REPORTERED AND MAKE MARKE ADD-MO-MON-MON TENTED	

图 8-5

点击立即进入后可进入回话,在会话协同中,可像分享人申请控制权,分享人同意后,便可对该会话进行操作。如图 8-6。



图 8-6

注意事项:

1. 当没有控制权的用户申请并且获得会话控制权,此时分享者可强制获取控制权。

2. 当创建者取消分享或者是退出当前会话时候,协同用户被踢出会话,且之前的会话链接失效。

3. 当协同者拥有控制权限时,可以点击【释放控制】,会话的控制权限会回到创建者手中。

#### 8.1.4 H5 登录图形协议主机

进入主机运维,登录 RDP、VNC 或应用发布资源,图形协议类型主机 h5 会话的登录,支持文件传输。与 SSH 类似,区别在于 RDP 的目标地址只有:主机网盘,支持下载网盘文件到本地,支持上传本地文件到网盘。如图 8-7。



图 8-7

注:图形协议会话的协同分享与字符类型协议的会话协同操作相同。

#### 8.1.5 SSH 客户端登录

通过 SSH 客户端登录堡垒机,此处以 xshell 为例。可新建会话如图 1-8, 主机为堡垒机 IP 地址, 默认端口为 22222, 点击连接后输入堡垒机账户密码即可登录成功。

可通过命令行输入登录堡垒机,登录用户名格式为【堡垒机用户@IP 地址端口号】登录 密码为堡垒机密码,登录到堡垒机后可选择资源标号登录堡垒机纳管内的账户。如图 8-8

	🚰 Session Options - 旗舰版堡垒机
Category: Connection Logon Actions SFTP Session Advanced Port Forwarding Remote/X11 Terminal Emulation Modes Emacs Mapped Keys Advanced	SSH2 Hostname: 106.75.134.203 堡垒机地址 Port: 22222 堡垒机客户端服务端口 Firewall: None ② Username: admin 堡垒机用户名 Authentication ✓ PublicKey ✓ Reyboard Interactive ✓ Password ✓ GSSAPI
Window Log File Printing X/Y/Zmodem	Key exchange <ul> <li>ecdh-sha2-nistp521</li> <li>ecdh-sha2-nistp384</li> <li>ecdh-sha2-nistp256</li> <li>diffie-hellman-group14</li> <li>diffie-hellman-group-exchange-sha256</li> </ul> Minimum group exchange prime size:       2048
	Cancel

图 8-8

注意事项:

支持使用 API 的登录方式登录堡垒机指定的资源登录账户,可直接通过命令行输 入:堡垒机账号@从账号@从账号 IP@堡垒机 IP 端口号,例如 admin@root@192.168.1.1@192.168.1.2 端口号,最后输入堡垒机密码,即可通过堡垒机登录 到指定的主机资源内。

### 8.1.6 SFTP/FTP 客户端登录

堡垒机支持登录 SFTP/FTP 协议类型主机,登录信息在主机运维中点击 SFTP/FTP 主机登录弹窗获取,在 SFTP/SFTP 客户端填写该登录信息即可成功登陆。此处以 FTP 为例,SFTP 类 似,区别是 SFTP 使用的是堡垒机密码,非明文密码,且无 URL 链接。如图 8-9。

(iii) U(	CLOUD									🛓 🗐 💭 admin 👻
			/ 主机运维	登录			×			
m		主机运维	ŧ	打开本地F	FP客户端,使用如下信	息登录			C Webž	四
		自动识别		服务器地址:	106.75.134.203					
۲			≠机杂款 ▲	端口:	2121				资源账户 💌	操作
۲			自建数据库	用户名:	admin@10.13.73.92				root	登录
ŵ			数据库审计-跳板	密码:	xj1xflbjzm9BcYPqs9	t0p1t5wTtl977tTNbl33lCv_vnklQx	7DWzSF		adminis 🔻	登录
			广州-UDB		夏制				root 📼	登录
			windows测试机	您也可以复	制以下URL并粘贴到F	TP客户端地址栏			adminis 💌	登录
	脚太管理		Windows测试内网	ftp://admi	n@10.13.73.92:xj1xflbjzm	9BcYPqs9t0p1t5v 复制URL			adminis 💌	登录
			Windows-内网-测						adminis 💌	登录
	快速运维		sftp-Linux-内网			取消	确定		root	登录
			Linux内网-测试机	10.13.48.217:22	SSH				root 📼	登录
崮				10.13.48.217:5901	VNC				root	登录
Bì										
۲										
		- E3	1/9项 批量到	2录 添加标签 删除	标签			,	9条 20条/页 👻	〈 1 〉 前往 1 页

图 8-9

注意:

1 支持的 SFTP/FTP 客户端种类: Xftp, WinSCP,FlashFXP, FileZilla。

2 其中 FTP 可复制 URL 到 FTP 客户端直接登录。

#### 8.1.7 数据库客户端登录

用户被授权数据库资源后,进入到主机运维的列表页面,点击数据库资源的登录按钮,会 出现代理程序的询问弹窗,如图 8-10。

11 U	CLOUD									🛓 🗐 💭 admin 🗸
-	桌面		桌面 / 运约	推 / 主机运维						
.#	部门		主机运	维					C Webj	送 <b>打</b> 到 登 动 置 御 运
•	用户	~	自动识别	1 ▼ 摘入搜索项查询	Q					
۲	资源	~		主机名称 ♠	主机地址 ≑	14, 501	4 <sup></sup> Mr		资源账户 🔻	操作
۲	策略	~		自建数据库	106.75.179.170:3	登示 (3.2.14) 请法择一个案	× 	··· Z	root 🔍	登录
<b>.</b>	运维	^		数据库审计-别版机	106.75.156.92:3389	· Navicat	(Plane / C	🔟	adminis 🔻	登录
				广州-UDB	10.13.157.111:3306	⊂ mysql end ⊂ Mysql Admi	nistrator	··· Z	root 🔍	登录
	应用运维			windows测试机	10.13.73.92:21	7.84		🔟	adminis 🔻	登录
	脚本管理			Windows测试内网	10.13.73.92:23	1991.2		… ∠	adminis 🔻	登录
				Windows-内阿-测	10.13.73.92:3389	RDP		🖉	adminis 🔻	登录
	快速运弹			sftp-Linux-内网	10.13.48.217:22	SFTP		… ∠	root 👻	登录
	运维任务			Linux-内网-测试机	10.13.48.217:22	SSH		Z	root 🔫	登录
ä	审计	~		linux-vnc	10.13.48.217:5901	VINC		··· Z	root 💌	登录
È	工单	~								
蕶	系統	~								
		Ξ		<b>赴0/9項</b> 批量發	经最 添加标签 删	除标签		ŧ	է9条 20 <b>条</b> 页 ▼	〈 1 〉 前往 1 页

图 8-10

选择要使用登录的客户端工具即可完成数据库资源的登录进行运维,见图 8-11。

- Auricut II												
文件 查看	收藏夹	工具	窗口	帮助								
- <b>-</b>					<b>F</b> (-)						<b>I</b>	
<b>〒口</b> · · · · · · · · · · · · · · · · · · ·	田白	<b>±</b>	די   E	0 <b>0</b> 11回	J(x) 函数	事件	香泡		备份	计划	「「「」」	
□ <b>1</b> 27.0.0.	. 1-7003-mvsal	4×	7:143	///24		711	249	1648	PA 1/3	PLAN	沃土	
db_n	ame		X 3 384									•
📄 hu			➡ 打开表	曳 💬 设	计表 🎨 新	建表 🐌 🖩	11除表 💽 🖣	入向导 📑	导出向导			Q
📄 info	rmation_schem	na										
mysq.	1											
perf	ormance_schem	na										
Servi	er_cos _2020_02											
S user	2020 03											
xuej:	iao											
🗐 zzy												
10 数据库				127.0	. 0. 1-7003-m	ysql 用)	È: root					≡ #

图 8-11

### 8.1.8 MSTSC 登录

堡垒机上添加 Windows 资源,用户被授权该资源后,支持在本地电脑上使用 mstsc 客户 端能连接运维资源。填写方式,计算机名:堡垒机 IP 地址: 53389。用户名:堡垒机用户名@ 运维的 windows 资源账户名@运维资源 IP 地址: 3389。然后在资源新弹窗页面输入堡垒机密 码。

	近边	程桌面 接					,
常规	显示	本地资源	体验	高级			
· 景登	2音	入沅程计管机	的夕称				
U,	ans ئات	角机(C):	192.1	° 68.1.184:53389		~	
	用	户名:	(IAZI1	11\administrator@	192.168.1.3	5:3389	
	ä	你连接时将向	同你询问	凭据。			
		允许我保存:	凭据(R)				
连接证	日本	当前 <mark>连接设置</mark>	星保存到	RDP 文件或打开—	已保存的道	<b>接</b> 。	
		保存(S)		另存为(V)	打开	Ŧ(E)	
●障痛	选项(O)			连	接(N)	帮助(	H)

图 8-12

- 192.168.1.184:53389 - 远程桌面连接	<u></u>	×
		^
*		
Login		
admin@YUNXIAZI111\adr	ninistra	
password <del>www</del>	机的密码	
OK Car	ncel	
3		
a		
		<b>-</b>
₹ 757222. ******		 <b>&gt;</b>

图 8-13





图 8-14

审计页面查看:

	桌面	di.	1 / 审计	/ 实时会语							
di.	ണ	3	如会话								
2	用户		资源名称	▼ 输入搜索项查询		R					
	an a			资源名称	後世々	主机应用地址	资源陈卢	用户	來應IP	开始时间 🖕	会活时长 🗅
	策略			uqVloQ	RDP	192.168.1.35	YUNXIAZI111\admin	admin	192.168.20.49	2020-05-20 16:35:23	00:00:26
	运维										
	审计										
	<del>文时会话</del> 历史会话										
	<u>業計会活</u> 历史会话 系統日志										
	<b>二时会话</b> 历史会话 系统日志 运 <del>维报表</del>										
	★ 計会活 历史会活 系統日志 运维报表 系統报表										
	<del>太計会活</del> 历史会话 系統日志 运筆报表 系統服表 工单										

图 8-15

#### 8.1.9 Web 运维配置

Web 运维配置支持一些特殊设定,支持的设定项有: admin console 选项,当 rdp 资源上的的远程服务器授权过期时无法登陆,勾选此选项能够强制登录进入资源,如图 8-16 所示;

Web运维	配置		$\times$
RDP			
	连接模式:	admin console	
			取消 确定
		图 8-16	

8.2 应用运维

进入[运维/应用运维],点击<登录>,可直接登录应用发布进入 H5 会话页面。如图 8-17。

10 U	ดนอ								4		Q <sup>®</sup> admin   ⊸
-	桌面		桌面 / 运维 / 应用)	云维							
đ.	部门		应用运维								0
Ŧ	用户	~	自动识别 🔻 😫	入搜索项查询	٩						
۲	资源	~	应用名和	R \$ 1	应用地址 ⇔	协议 👻	标签 🗸		资源账户 🔻	操作	
•	策略	~	chrome			Chrome		··· _	adminis 🔻	登录	
Ψ	运维	^									
	主机运维										
	脚本管理										
	快速运维										
	运维任务										
ä	审计	~									
Ē	工单	~									
-	系统	, II	已进0/1項	添加标签	删除标签			¥	1条 20条/页 🔻	(1)	前往 1 页

图 8-17

注意事项: 支持回话协同分享, 此处会话协同操作与字符类型会话协同操作相同。

### 8.3 脚本管理

脚本用于执行快速运维和运维任务时添加脚本使用,进入脚本管理页面,可查看当前用户 所创建的脚本,支持在线编辑或导入格式为 Python 和 shell 格式的脚本。如图 8-18。

121 U							_				⊥ 🗉	Q <sup>69</sup> admin 👻
			/ 脚本管理	新建脚本			×					
ħ		脚本管理	E		来源:	<ul> <li>在线编辑</li> <li>文件导入</li> </ul>						O 新建
*		脚本名称			* 名称:							
۲			脚本名称 ⇔			长度1-64个汉字或字符,允许输入汉字、 字母、数字、"-"或"."		操作				
۲			rz-sz		类型:	• python Shell		管理	下载	删除		
m			命令测试			类型指定后不可修改		管理	下载	删除		
					描述:							
						描述最长128个汉字或字符						
							取消 确定					
Ш												
B												
\$			0/2项					共 2 条	20 条/	<b>页</b> 💌	< 1. >	前往 1 页

图 8-18

注意事项: 脚本属于个人空间, 所有的脚本详情仅限创建者可见。

### 8.4 快速运维

进入快速运维模块,可看到相应的 tab,选择需要执行的账户,便可在该账户快速执行命 令,脚本和传输文件,执行完成后可在执行日志中查看详情信息。如图 8-19。

								↓ 🗉	💭 admin 🔻
Ŧ	桌面		桌面 / 运维 / 快速运维						
ф.	部门		快速运维						0
1	用户	~	命令控制台 脚本控制台	文件传输控制台 执行日志	3				
۲	资源	~							
٢	策略	~	* 执行命令:	ls	立即	<b>执行</b> 中断执行			
щ.	运维	^	* 执行账户:	⊥ root@Linux-内网-测试机					
	主机运维			亦 - **** <b>王帝</b>					
	应用运维			四行 重量					
	脚本管理		更多选项:	□ 提权执行					
	运维任务		自动识别 👻 输入搜索项音	询 Q					會用
É	审计	~	时间	主机名称	主机地址	执行账户	执行状态 🔻	执行结果	
	丁鱼	~	2020-02-10 16:50:18	海盟堡壘機測試	152.32.186.13	user001	不可达	展开	
_	 7/#	~	2020-02-10 16:50:18	Linux-内网-测试机	10.13.48.217	root	成功	展开	
~	杀犹	× .							

图 8-19

注意:

当该执行账户在主机的 sudoers 文件夹中时,便可勾选提权执行,执行相应命令。

### 8.5 运维任务

=

进入运维任务模块,可新建运维任务,执行方式可选择手动执行,定时执行,周期执行, 更多选项可勾选提权执行,点击<下一步>选择要执行的账户。如图 8-20。

🖾 υςτοπρ						上 🗐 💭 admin 💌
- 桌面	桌面 / 运维 / <b>运维任务</b>	新建运维任务		$\times$		
<b>山</b> 部门	运维任务	* 任务名称:				O Mill
上 用户 ~	任务列表 执行日志		长度1-64个汉字或字符,允许输入英文字 母、数字、或""			
◆ 资源	任务名称 👻 输入授業项查询	* 执行方式:	手动执行			
策略 ~	任务名称 *	要多选项:	標和地行		执行结果	操作
型 运维 へ		2.2.2.2.	BERRATI			
主机运维		任务描述:				
应用运维			描述最长128个汉字或字符			
脚本管理						
快速运维				取消 下一步		
运维任务						
<b>首</b> 审计 ~						
<b>В</b> Т# ~						
▼ 系统	□ 已选0/0项					

图 8-20

执行账户选择完成之后可添加任务步骤,步骤可选择执行命令,执行脚本,文件传输。支持添加多个步骤。如图 8-21。

E U							. ↓ 🗉	admin 🔻
-		桌面 / 运维 / <b>运维任务</b>	新建运维任务		×			
æ		运维任务	步骤1	删除 添加任	务步骤 🔻			0 <b>新達</b>
*		任务列表 执行日志		执行	命令			
۲		<u> </u>	* 步骤名称:	请输入步骤名称 执行服 长度1-64个汉字或字符、允许输入英文字	脚本			
۲				母、数字、或"" 传输:	文件			
щ.		任务名称	* 执行命令:	请输入执行的命令及参数	1	行结果	梟作	
				10 2 -J 2 2 17 I I I I I I I I I I I I I I I I I I				
	脚本管理			取消上一步	テ 确定			
	快速运维							
Ű								
Bì								
•		□ 已送0/0项						

图 8-21

### 9 审计

## 9.1 实时会话

实时会话可查看当前时间正在运维的会话,对于字符类型协议和图形协议的 H5 运维可进 行实时监控,对于客户端登录的协议,可在详情中查看运维记录 (SSH 协议客户端运维可查看 实时会话),在会话过程中,管理员可以强制中断该回话。如图 9-1

យប												<u>↓</u> 🗏	🔎 admin 👻
Ŧ	桌面		桌面 / 审	计 / 实时会话									
.m.	部门		实时会	·话									0
•	用户	~	资源名	秋 ▼ 输入搜;	素项查询	Q 高级搜索							
۲	资源	~		资源名称	类型 👻	主机/应用地址	资源账户	用户	来源IP	开始时间 💠	会话时长 ⇔	操作	
9	策略	~		Linux-内	SSH	10.13.48.217	root	admin	183.238.1	2021-04-25 16:52	00:00:03	详情 监控	中断
ŵ	运维	~											
Ň	审计	^											
	实时会话												
	历史会话												
	系统日志												
	运维报表												
	系统报表												
Ē	工单	~											
\$	系统	* E	B	选0/1项	中断					共	1条 20条/页 💌		前往 1 页

图 9-1

### 9.2 历史会话

当会话结束后,可在历史会话中查看该会话中所有操作,字符类型协议和图形协议可播放 视频,且支持将会话文件下载到本地进行播放。对于在客户端登录的会话, SSH 客户端同样支 持下载会话文件进行播放,其他客户端会话不支持播放,仅能在详情查看运维。如图 9-2

11 U												<u> </u>	🗉 🗘 🗐 admin 👻
-	桌面		桌面 / 1	审计 / 历史会词	Ĩ								
đ	部门		历史会	话									0
•	用户	~	资源名	「称 マ 輸入」	搜索项查询	Q. 高級搜護	家						导出
۲	资源	~		资源名称	类型 👻	主机/应用地址	资源账户	用户	来源IP	起止时间 💠	会话时长 🜲	结束状态 👻	操作
9	策略	~		Linux	SSH	10.13.48.217	root	admin	183.23	2021-04-25 10:	00:38:43	正常结束	详情 播放 下载
Ψ.	运维	~		Linux	SSH	10.13.48.217	root	admin	183.23	2021-04-25 10:	00:11:49	正常结束	详情 播放 下载
Ë	审计	^		Linux	SSH	10.13.48.217	root	admin	183.23	2021-04-23 15:	00:52:06	正常结束	详情 播放 下载
	实时会话			数据库	RDP	106.75.156.92	adminis	admin	183.23	2021-04-09 10:	01:24:32	正常结束	详情 播放 下载
	历史会话			数据库	RDP	106.75.156.92	adminis	admin	183.23	2021-04-09 10:	00:00:43	正常结束	详情 播放 下载
	石体口士			sftp-Li	SFTP	10.13.48.217	root	admin	106.75	2021-04-09 10:	10:00:19	强制中断	详情 播放 下载
	杀鈗日志			Linux	SSH	10.13.48.217	root	admin	183.23	2021-04-06 11:	00:07:47	正常结束	详情 播放 下载
	运维报表			Linux	SSH	10.13.48.217	root	admin	183.23	2021-04-01 18:	00:35:46	正常结束	详情 播放 下载
	系统报表			数据库	RDP	106.75.156.92	adminis	admin	183.23	2021-03-31 18:1	00:06:08	正常结束	详情 播放 下载
B	工单	~		数据库	RDP	106.75.156.92	adminis	admin	106.75	2021-03-31 18:	00:00:06	正常结束	详情 播放 下载
-	系统	> III	E	已选0/20项	1				1.	共 152 条 20 条/页	<ul> <li>✓ 1 2</li> </ul>	3 4 5 6	8 〉 前往 1 页

图 9-2

## 9.3 系统日志

系统日志可查看用户登录系统的日志以及所有操作的日志,进入系统日志页面后,可看到 两个 tab。系统登录日志可查看堡垒机用户的登录日志。系统操作日志可查看堡垒机用户的操 作日志。可导出日志。如图 9-3

11 U	CLOUD									↓ 国	Q <sup>8</sup> admin 👻
-	桌面		桌面 / 审i	计 / 系统日志							
.m.	部门		系统日編	志							0
₹	用户	~	系统登录	日志 系统操作日志							
۲	资源	~	用户	▼ 输入搜索项查询	〇. 高级搜索	2					导出
9	策略	~		时间 ⇔	用户	来源IP	日志内容	登录方式 💌	结果 💌	备注	
Ţ	运维	~		2021-04-25 16:46:59	admin	183.238.16.138	登录系统	Web页面	成功	-	
Ĩ	审计	^		2021-04-25 12:24:44	admin	183.238.16.138	退出系统	Web页面	成功	-	
	实时会话			2021-04-25 11:32:10	admin	183.238.16.138	登录系统	Web页面	成功	-	
	历史会话			2021-04-25 11:32:02	admin	183.238.16.138	登录系统	Web页面	失敗	登录系统,密码错误	
				2021-04-25 11:14:48	admin	183.238.16.138	退出系统	Web页面	成功	-	
	运维报表			2021-04-25 09:47:05	admin	183.238.16.138	登录系统	Web页面	成功	-	
	系统报表			2021-04-25 08:34:	lixin	220.174.25.172	登录系统	SSH客户端	失败	登录系统,密码错误	
Ĩ.	工单	~		2021-04-25 08:34:	lixin	220.174.25.172	登录系统	SSH客户端	失败	登录系统,密码错误	
-	系统	, E	- ex	<b>选0/20</b> 项			共 229297 务	€ 20条/页 ▼	< 1 2 3	4 5 6 … 11465 >	前往 1 页

图 9-3

系统日志导出包括系统登录日志导出和系统操作日志导出,系统日志导出时间限制在 180 天以 内,支持导出时间范围选择,如图 9-4

	CLOUD													٩				<u> </u>	Q <sup>8</sup> admin ⇒
				十 / 系统日志	导出								×	I					
ф			系统日調	5	* #2 it at (a)									I					0
<u>.</u>		~	系统登录	日志 系统操作日志	** #FTT#310)-	2021-03-25	~2021-0	4-25											
۲		~				~ ~ ~	2021 :	申3月	Ŧ	~			2021	1 24 4	月	>	>> 		
		<u> </u>	用户			28 1	2 0	3 4	5	6	28		30	31	1	2	3		与出
, v				时间 💠	用户	7 8	9 1	0 11	12	13	4	5	6	7	8	9	10	备注	
m		~		2021-04-25 16:46:59	admin	14 15	16 1	7 18	19 3	20	11	12	13	14	15	16	17	-	
É		~				21 22	23 2	4 25	26	27	18	19	20	21	22	23	24		
				2021-04-25 12:24:44	admin	28 29	30 3	1 1			今天	26	27	28	29	30		-	
				2021-04-25 11:32:10	admin	4 5												-	
				2021-04-25 11:32:02	admin	183.238.16.1	138	登录	系統		V	/eb页值	i		失测	<u>4</u>		登录系统,密码错误	
				2021-04-25 11:14:48	admin	183.238.16.1	138	退出	系统		v	/eb页面			成功	b			
				2021-04-25 09:47:05	admin	183.238.16.1	138	登录	系统		v	Veb页面			成1	ħ			
				2021-04-25 08:34:	lixin	220.174.25.1	172	登录	系统		s	SH客户	鏰		失则	¢		登录系统,密码错误	
Ē		~		2021-04-25 08:34:	lixin	220.174.25.1	172	登录	系统		s	SH客户	蠕		失则	<u>y</u>		登录系统,密码错误	
-		× 		10/20项					<del>,</del>	229297	条	20 条/0	τ		<	1	2 3	4 5 6 … 11465 >	前往 1 页

图 9-4

### 9.4 运维报表

进入运维报表,点击要查看的 tab,可查看运维相关报表内容。支持导出报表到本 地。如图 9-5



图 9-5

## 9.5 系统报表



地。如图 9-5

进入系统报表,点击要查看的 tab,可查看系统相关报表内容。支持导出报表到本

图 9-5

# 9.6 报表自动发送

当开启报表自动发送,会按勾选的发送时间定时发送报表至邮件。如图 9-6

(ii) U					💭 admin 👻
		桌面 / 审计 / <b>运维报表</b>	报表自动发送	×	
'n		运维报表	状态:	○ 报表自动发送	报表导出
*		运维时间分布 运维Top分析		开启后,在每个周期开始时,系统将会自动 生成上一周期的运维报表,并以邮件形式发 进	
۲		趋势图	10.544 775447		
۲		2020-08-01-2020-12-31	友达周期;	<ul> <li>○ 毎日 毎日00:00次送</li> <li>○ 毎周 毎周-00:00次送</li> </ul>	
ŵ				☑ 每月 每月一日00:00发送	
Ű			文件格式:		
				取消	
Bì				admin	
-					

图 9-6

第53页共89页

## 10 工单

### 10.1 访问授权工单

访问授权工单用于运维员不具备运维某台主机资源权限,且又需要运维该资源时,可通过 访问授权工单申请访问资源。点击新建访问授权工单,可选择自己要运维的时间和自己需要的 功能。如图 10-1

(2) U									⊥ 🗉 🗘 a	dmin 🤝
-		桌面 / 工单 / 访问:	新建访问授权工单				×			
.m.		访问授权工单	* 法辨时间:	生物时间	di: 86 Rt (61				0	新建
<u>.</u>		工単号 👻 新	100 Page 2012							
۲		THE	文件传输:	✓ 上传 ✓ 下載				18.4x		
۲		20200100	更多选项:	✓ 文件管理 ✓ 上行剪切板	🛃 下行剪切板	🛃 显示水印		管理 提交	軍家	
ŵ			工单备注:					10-1 10-14	<b>T</b> 2	
Ű								10.54 30.55	2.9 W.A	
B				音注最长128个汉子或学行				管理 强父	史多	
							取消下一步	管理提交	更多	
		20190704	11710-101000207	10261	di	-		管理提交	更多	
•										
		□ 已选0/5项					,	5条 20条/页	< 1 > 前往	1 页

图 10-1

最后选择要运维的资源主机,勾选立即提交后该工单会自动提交,否则需要在访问授权工 单模块进行手动提交。管理员审批通过后该工单生效。如图 10-2

11 U	CLOUD							🛓 🗉 🗘	admin 📼
			桌面 / 工单 / 访问	问授权工单	新建访问授权工单				
æ			访问授权工单		关联资源账户 关联账户组				新建
.≖		~	工单号 📼	输入搜索项查询					
۲		~	T#R		可选择的资源账户	已选择的资源账户	单备注	操作	
۲		~		081711152346136	请输入关键词查询 Q.	请输入关键词查询 Q	The state of the s	管理 提交 更多	
m		~		011038184735125	□ 目建数据库 / 106.75.179 □ administrator Windows-内网-测试机 /	□ 目建数据库 / 106.75.179		管理 损交 更多	
Ë		~		221719577909524	UEmpty] Windows-内网-测试机 /			管理 提交 更多	
B		^		221719579502878	sftp-Linux-内网 / 10.13.48.217			管理 提交 更多	
				04144943460320'	sftp-Linux-内网 / 10.13 administrator windows测试机 / 10.13.7			管理 损交 更多	
					root linux-vnc / 10.13.48.217				
					□ 共 21 项	□ 共1项			
					是否立即提交				
~		~				取消 上一步 确定			
		Ξ	□ 已选0/5项	删除			共 5 券	▲ 20条/页 ▼ < 1 > 前往	1 页

图 10-2

#### 【工单克隆】

如果需要再次使用申请过得资源,可以使用工单克隆功能快速复制工单,如图 10-3,点击更多即可看到克隆功能

11 U	CLOUD								🛓 🗐 🎝 admin 👻
Ŧ	桌面		桌面 / エ	单 / 访问授权工单					
đ	部门		访问授	权工单					C Sti SH
•	用户	~	工单号	▼ 输入搜索项查询	Q. 高级搜索				
۲	资源	~		工单号	状态 🔻	申请时间 💠	资源账户	工单备注	操作
9	策略	~		202001081711152346136	已撤回	2020-01-08 17:11:15	± = m =	-	管理 提交 更多
m	运维	ř		201911011038184735125	审批中	2019-11-01 10:38:18	± - m -	-	管理 提交 撤回
Ě	审计	Ý		201910221719577909524	审批中	2019-10-22 17:19:57	王 - 赤 C组	-	克隆 管理 提交 删除
Ē	工单	^		201910221719579502878	审批中	2019-10-22 17:19:57	± - m -	-	管理 提交 更多
	访问授权工甲			201907041449434603207	待完善	2019-07-04 14:49:43	± - m -	-	管理 提交 更多
	中文 (文代上平 教 編 広 編 初 丁 音								
	丁单审批								
•	<u>工</u> 二十 二 九 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	~							
		Ē	E	选0/5项 删除				共 5 条	· 20 条/页 🔍 🤇 1 🔪 前往 1 页

图 10-3

注意: 除了待完善状态的工单都能进行复制

# 10.2 命令授权工单

管理员为用户配置命令控制策略后,当用户登录该资源并执行了策略中的命令,命令授权 工单列表中就会自动生成一个命令授权工单。如图 10-4。



图 10-4

如果 admin 在系统配置中的命令授权工单提交方式配置为手动提交,则需要在命令授权工 单中手动点击提交,管理员审批同意后,刷新页面,该工单生效。如图 10-5。

11 U										<u>↓</u> 🗏	Q <sup>12</sup> admin 👻
-	桌面		桌面 / 工单	/ 命令授权工单							
.m.	部门		命令授权	工单							0
₽	用户	~	工单号	▼ 输入搜索项查询	Q ( )	级搜索					
۲	资源	~		工单号	状态 👻	申请时间 💠	执行命令	资源账户	工单备注	操作	
9	策略	~		20210425170344596	待提交	-	SZ	⊥ root@Linu	-	管理 撤回 提交 删除	
m	运维	~									
Ŭ	审计	~									
Ē	工単	^									
	访问授权工单										
	命令授权工单										
	数据库授权工的	单									
	工单审批										
~	系统	~									
		Ē	- E30	0/1項					共1条	20条页 👻 🤇 1 🗦	前往 1 页

图 10-5

注意事项:

命令授权工单由用户触发"动态授权"命令策略时自动创建,无法手动创建命令授权工单。

### 10.3 数据库授权工单

管理员为用户配置数据库控制策略并添加相应的规则后,当用户登录该资源并执行了策略 中的规则,数据授权工单列表中就会自动生成工单,点击提交,管理员审批通过后状态为生 效。如图 10-6。

-	skin		東西 / 工単	1 / 数据库授权工单							
.m.	部门		数据库报	受权工单							0
•	用户 、	~	工单号	▼ 輸入投資資源例 Q	毫级搜索						
۲	資源	~		工单号	状态 🔻	申请时间 \$	90.01	资源账户	工单备注	操作	
ø	第略	~		201910111701279864067	待损交		库=123123; 命令=select	⊥ root@mysql		管理 彩回 揭交 删除	
ŵ	运维	~		201910111701552544372	待损交		库=123123; 表=123; 命令	⊥ root@mysql		管理 影回 提交 勤除	
Ŭ	审计 、	~									
B	1# ·	~									
	访问授权工单										
	命令授权工单										
	工单审批										
\$	系统	~									
			Bis	50/27R IIII0						共2条 50条页 💌 🔇 🚺 为 前	佳 1 页
	=										

图 10-6

注意事项:

1 如果系统配置中命令授权工单配置为手动提交,则需要手动提交给管理员,管理员同意
 后,该工单生效。

2 目前数据库授权工单只支持 MySQL 和 oracle 两种数据库。

3 数据库授权工单由用户触发"动态授权"命令策略时自动创建,无法手动创建数据库授 权工单。

#### 10.4 工单审批

工单审批用于对堡垒机用户提交后的工单进行审批,进入工单审批后可查看当前需要审批 和审批后的工单,点击管理可查看审批人节点,和审批内容。支持勾选后批量审批。如图 10-7

11 U	CLOUD										<u>↓</u> ■	Q <sup>12</sup> admin 👻
Ŧ	桌面		桌面 / 工年	1 / 工单审批								
÷.	部门		工单审批	t								0
Ŧ	用户		工单号	▼ 输入搜索项查询	<u>्</u> र	极搜索						
۲	资源			工单号	工单状态 🔻	申请时间 💠	工单类型 🔻	申请内容	创建者	操作		
0	策略			201910221719577909	审批中	2019-10-22	访问授权	王 - 山 C细	admin	管理 批准 驳	回 撤销	
Ψ.	运维			201910221719579502	审批中	2019-10-22	访问授权	* = m =	admin	管理 批准 驳	回 撤销	
Ë	审计			201906142100381319	已过期	2019-06-14	访问授权	* - m -	admin	管理批准驳	撤销	
Ē	工単			201809301605135541	已撤销	2018-09-30	访问授权	* - m -	admin	管理批准 驳		
	访问授权工单											
	命令授权工单											
	数据库授权工!	单										
	工单审批											
蕶	系统											
		E	- C3	10/4項 批准					共 4 条	20 条/页 🔍	< 1 >	前往 1 页

图 10-7

## 11 系统

### 11.1 安全配置

#### 11.1.1 用户锁定配置

用户锁定配置的锁定方式是指输错密码达到尝试密码次数被锁定的方式,有账户和来源 IP 两种方式,尝试密码次数是指可以输错密码的次数,如果设置为 0,则不锁定账户/来源 IP, 默认值 5 次。锁定时长是指用户输错密码被锁定的时长,如果设置为 0,则锁定账户/来源 IP 直到管理员解除。重置计数器时长指的是登录尝试密码失败后,将登录尝试失败计数器重置为 0 次所需要的时间,默认值 5 分钟。如图 11-1



图 11-1

### 11.1.2 密码策略配置

密码策略配置中密码强度校验开启后更改密码时不得更改为简单密码。新用户强制改密打 开后,当用户第一次登陆到堡垒机时,系统强制用户更改堡垒机密码。密码相同校验是指,更 改密码时不得与前 x 次的密码相同,默认为 5 次。密码修改周期默认为 30 天,当到达 30 天后系统会强制堡垒机用户更改密码。如图 11-2

									⊥ I Q <sup>12</sup> admin -
-			桌面 / 系统 / <b>系统配置</b>		密码策略配置		×		
			系统配置		密码强度校验:				
		~	安全配置网络配置	HAB		开启强密码校验,密码长度为8-32个字符, 数字和特殊字符,不支持空格	且包含大小写字母、	系统风格	
		~	用户锁定配置		新用户强制改密:				∠ 编辑 ※
		~				平地以並用广目以互求於机构必须涉以否约			
		~	镇定方式:	用户	* 密码相同校验:	1 有效值1-30。检查新密码不能与前N次设置	次		
		~	尝试密码次数:	0次		的密码相同,N默认值为5			
<b>Fi</b>	工商	~	银定时长:	30分	* 密码修改周期:	0	Ŧ		
		^	重置计数器时长:	5分钟		有效值0-90。如果设置为0,则用户密码 永不过期,否则当达到修改周期后须修改密码,默认值为30			
			密码策略配置				取消 确定		∠ 编辑 《
			密码强度校验:	禁用					
			密码相同校验:	1次					
			新用户强制改密:	禁用					
		Ξ	密码修改周期:	0天					

图 11-2

## 11.1.3 web 登录配置

Web 登录配置中登录超时默认为 30 分钟, 当登录堡垒机 30 分钟后页面无任何操作则需 要重新登录堡垒机, 短信验证码过期时间默认为 60 秒, 当使用手机短信登录接收的验证码在 60 秒之内有效。支持更改 USBkey 类型。当开启图形验证码为自动时, web 登录页面输入密 码错误超过 3 次则会出现验证码, 验证码过期时间默认为 60 秒。当开启域控校验时用户登录 时需要进行域控校验, 且用户的新建和编辑弹窗增加"更多选项:域控校验"复选框的展示。 如图 11-3



图 11-3

#### 11.1.4 web 证书配置

在 web 证书配置中可上传正确格式的证书文件, 输入密码后即可。如图 11-4

11 U	CLOUD				👱 🗉 Q <sup>12</sup> admin -	r
			桌面 / 系统 / <b>系统配置</b>	Web证书配置	×	
ħ			系统配置	卜传证书文件:	点走上传	
*		~	安全配置 网络配置	HAT	调上传Tomcat køystore格式证书文件,大小不超过10MB 系统风格	
۲		~		★ keystore密码;		
۲		~	Web证书配置		∠ 编辑 《	
œ		~			取消	
崮		~	常用名称:	*.uhasadmin.com		
B		~	签发者:	GeoTrust CN RSA CA G1		
۲		^	过期时间:	Oct 13 12:00:00 2022 GMT		
			客户端登录配置		∠ 编辑 《	
			登录超时:	600分钟		
			SSH公钥登录:	启用		
		=	SSH密码登录:	启用		

图 11-4

#### 11.1.5 客户端登录配置

SSH 登录超时默认为 30 分钟,当在客户端登录堡垒机之后 30 分钟无操作,再次操作需要重新登录。当开启 SSH 公钥登录并用户配置了 SSH 公钥即可免密码登录。密码登录开启后在 SSH 客户端登录时只能输入密码登录,如公钥登录和密码登录全部开启,则优先使用公钥登录。如图 11-5

(II) U (II)							. ⊥ 🗉 🗘	admin 👻
		桌面 / 系统 / <b>系统配置</b>	客户端登录配置		×			
æ		系统配置	* 晋录招时:	600	分钟			
*		安全配置 网络配置	HA	有效值1-43200。当用户超过设定时长无 操作时,再次操作需要重新登录,默认值为	9	系统风格		
۲		客户端登录配置		30			1	编辑
Ø			SSH公钥登录:					
ŵ		登录超时:	600: SSH密码登录:					
崮		SSH公钥登录:	启用					
Đ		SSH密码登录:	启用		取消 确定			
		登录方式配置					∠ \$	编辑 😞
		默认登录方式:	手机短信,密码登录,手机令牌,し	ISB Key,动态令牌				
		USB Key配置					∠ \$	扁锥  ≪
		USB Key:	龙脉科技					

图 11-5

## 11.1.6 USB Key 配置

USB Key 类型包含龙脉科技、北京 CA、海泰方圆、鱼翁、吉大正元可配置。更改之后用 户签发 USB Key、用户使用 USB Key 方式登录也做相应的变化。如图 11-6、图 11-7

11 U			<u>↓</u> ■	Q <sup>12</sup> adm	in 👻
Ŧ		点回 / 系统 / 系統配置 USB Key配置 ×			
ŵ		系统配置 USBKey: 分缺版件			
*		安全配置         网络配置         HAE         切りUSB Keyg型掺合导致之前差发的         系统风格           USB Key无法使用         USB Key无法使用 </th <th></th> <th></th> <th></th>			
۲				/ 编辑	
٢		取消 确定			
m		默认量录方式: 手机提信,密码量录,手机令牌,USB Key,动态令牌			
崮					
B		USB Key配置		∠ 编辑	
۰		USB Key: 龙脉科技			
		手机令牌配置		∠ 编辑	
		类型: 內置手机令牌			
	Ξ	根证书列表	〇〇 双向认证	+ 添加	

图 11-6

		桌面 / 系统 / <b>系统配置</b>	USB Key配置						
ά		系统配置	USBKey:	吉大正元	•				
*	~	安全配置 网络配置 HA		切换USB Key类型将会导致之前签 USB Key无法使用	无发的	系统风格			
۲	~	默认登录方式: 手机	* 服务器地址:						
۲	~			请输入服务器地址					
m	~	USB Key配置	+ APP ID:					∠ 编辑	
Ü	~	USB Key: 龙脉							
	~			_	取消 确定				
•	^	手机令牌配置						∠ 编辑	
		类型: 内置	手机令牌						
		根征共利率					网络拉莱		
		T IKE INVER							
	æ	序列号 颜	发给	质发者 起	始时间 🗢	截止时间 令	操作		

图 11-7

### 11.1.7 手机令牌配置

堡垒机除了使用内置的手机令牌,还支持使用奇安信 ID 或 Radius 令牌, 见图 11-8 和图 11-9,选取对应的类型后将数据填写进入并保存,用户就可以 在登录时使用对应的手机令牌服务。

						-	⊥ 🗐 💭 🔁 admin 👻
Ŧ		桌面 / 系统 / <b>系统配置</b>	手机令牌配置				
		系统配置	#5	。 内署王和今時			
	~	安全配置 网络配置	НАВ	内置手机令牌		系统风格	
	~	USB Key配置		奇安信ID	取消 确定		∠ 编辑 《
	×	USB Kev:	龙脉彩坊	RADIUS			
	~						
	~	┃手机令牌配置					∠ 编辑 《
	~						
	^	类型:	内置手机令牌				
		根址书列表					
		序列号	颁发给	颁发者	起始时间 令	截止时间 令	操作
					暂无数据		
	E						

图 11-8

### 11.2 网络配置

### 11.2.1 网络接口列表

其中网络接口列表可以编辑、删除当前机器的相关网络接口,为后续相关操作用到网络接口做准备 (删除不会删除机器中的相关接口,默认显示的网络接口不可以删除)。如图 11-10

C U	CLOUD													<u> </u>	II ( <sup>12</sup>	admin 👻
Ŧ	桌面		桌面 / 系统 /	系统配置												
ά	部门		系统配置													
Ŧ	用户	~	安全配置	网络配置	HA配置	端口配置	外发配置	认证配置	工单配置	告警配置	审计配置	系统风格				
۲	资源	~	网络接口列	表												*
0	策略	~	接口名称		Device		IP地址		子网掩码/前绸		速率		状态	操作		
Ψ	运维	~	eth0		eth0		10.13.61.147		255.255.0.0		-		up	配置		
Ë	审计	~					-		-							
iii	工单	~	DNS配置												∠ 编辑	*
	系统	^														
				首选DNS:	10.13.255.1											
	数据维护			备用DNS:	-											
	系统维护															
	关于系统		默认网关												∠ 编辑	*
		Ē		默认网关:	10.13.0.1(DH	ICP)										

图 11-10

### 11.2.2 DNS 配置

可修改当前机器的首选 DNS 和备用 DNS, 输入正确的 DNS 地址即可。如图 11-11

							<u>↓</u> E	D <sup>12</sup> adi	min 🤝
	桌面 / 系统 / <b>系统配置</b>	DNS配置		×					
	系统配置	* 首选DNS:	10.13.255.1						
	安全配置 网络配置	НАБ			系统风格				
	接口名称	香用DNS:				状态	操作		
	eth0	eth0		取消 确定		up	配置		
	DNS配置							∠ 编辑	
	首选DNS:	10.13.255.1							
	备用DNS:								
	Rept co 4							4 (048	
	▮ 款以两大							3844	
	默认网关:	10.13.0.1(DHCP)							
	IPv6的默认网关:								

图 11-11

### 11.2.3 默认网关

可在默认网关处修改 IPv4 和 IPv6 的默认网关。如图 11-12

(iii) (iii)							. ↓	D <sup>12</sup> admin	
		桌面 / 系统 / <b>系统配置</b>	编辑默认网关		×				
æ		系统配置	默认网关:	10.13.0.1					
*		安全配置 网络配置	НАВ	请配置正确的网关,否则可能会造成堡垒 无法连接	机	系统风格			
۲		DNS配置						∠ 编辑   《	
Ø			IPv6的默认网关:	请配置正确的网关,否则可能会造成堡垒	机				
ŵ		首选DNS:	10.15	无法连接					
崮		备用DNS:	-						
B		默认网关	_		цхля (нде			/ 编辑 /	
•									
		默认网关:	10.13.0.1(DHCP)						
		IPv6的默认网关:							
		静态路由配置					〇 刷	新 十 添加 🔹	
		目的地址	子网掩码/前缀	下一跳地址 路由类型	出口设备	Metric	备注	操作	

图 11-12

### 11.2.4 静态路由配置

可为当前机器添加静态路由, 使当前机器可以访问到其他网段的机器。如图 11-13

							<u> </u>	admin 👻
Ŧ		桌面 / 系统 / <b>系统配置</b>	添加静态路由		×			
		系统配置	继刑:					
		安全配置 网络配置 HAT				系统风格		
			* 目的地址:					
		默认网关: 10.13	* 子网掩码:					
		IPv6的默认网关: -	* 下一跳地址:					
		静态路由配置	出口设备:	eth0 ~				新+添加 <
		目的地址 子界	Metric:	1		Metric	备注	操作
						0		
		10.13.0.0 255	备注:			0		
		169.254.0.0 255				1002		
				_	- 與7月			
		OpenVPN配置						∠ 编辑 《
		服务器: -						

图 11-13

#### 11.2.5 OpenVPN 配置

堡垒机支持作为客户端连接到 OpenVPN 服务器,从而实现操作运维 VPN 内部资源的目的。点击开启并选择与本地 OpenVPN 服务器相同配置的协议、 IP、端口、是否压缩、验证 nsCertType 等信息,并上传 OpenVPN 服务器生成的 CA 证书,客户端证书和客户端私钥,填

写完成后即可将堡垒机添加到堡垒机服务器,用户可对 VPN 内部资源运维,审计等操作。如

图 11-14

111 U	CLOUD							<u> </u>	∃ Q <sup>12</sup> admin ▼
-			桌面 / 系统 / <b>系统配置</b>	OpenVPN配置		×			
æ			系统配置	<ul> <li>服务器地址:</li> </ul>					
*		~	安全配置 网络配置 HA		请输入有效的IP地址或域名		系统风格		
۲		~		* 端口:	1194				
۲		~	静态路田配置		请输入1-65535之间的有效数字				
Ţ.		~	目的地址子	协议:	TCP O UDP		Metric	备注	操作
É		~		) 压缩:			0		
Bì	工单	~	10.13.0.0 25	中断后重连:			0		
			169.254.0.0 25	6	_		1002		
~	杀鈗			验证nsCertType:					
			OpenVPN配置	CA证书文件:	点击上传				∠编辑 ≪
			服务器: -	客戶端证书文件:	点击上传				
			状态: 已書	客户端私钥文件:	点击上传				
		Ē				取消 确定			

图 11-14

#### 11.3 HA 配置

进入 HA 配置页面后可查看当前 HA 状态, 开启 HA 需要两台堡垒机, 并且版本一致, 点击启用后需要先配置主节点, 在备节点 IP 栏输入需要作为备节点的 IP, HAkey 可在堡垒 机的系统-关于系统中查看, 在浮动 IP 栏输入未被使用的 IP 地址, 浮动 IP 格式为地址/掩 码, 选择浮动 IP 网口和 HA 心跳接口点击确定后重启主节点 (未重启时状态为单机状态)。 重启完成后配置备节点, 配置完成后重启备节点即可。如图 11-15

(ii) U(	CLOUD							⊥ 🗉	Q <sup>12</sup> admin 👻
		桌面 / 系统 / <b>系统配置</b>		启用HA					
th		系统配置		热备初始角色:	○ 主节点 ○ 备节点				
<u>.</u>		安全配置 网络配置	HAā				系统风格		
۲		┃ 双机设备设置		* HA群组验证秘钥:	j05hpq3bdhug6csyfebv 请输入8-20位的有效数字或字母				
				* 备节点IP地址:					
m		HA状态:	禁用						
崮		当前运行状态:	单机	* 窗中点HA KEY:					
Ĩ.		浮动中地址:	-						
۲		热备初始角色:	主节	* 浮动IP地址:	IP地址/掩码位数,例如:				
		备节点IP地址:	-		192.168.1.100/24。请使用与主节点在同 一网段且未使用的IP地址				
		浮动IP网口:	-	浮动IP网口:	eth0 👻				
		HA心跳接口:	-	HA心跳接口:	eth0				
					取消	确定			

图 11-15

第66页共89页

## 11.4 端口配置

进入端口配置页面可查看当前端口, 共分为三种, 运维端口, web 控制台端口, SSH 控制 台端口, 运维段口配置主要针对 SSH/SFTP 和 FTP, 端口配置完成后重新启动堡垒机即可。如 图 11-16

11 U													<u> </u>	I (	adm	in 🔻
-	桌面		桌面 / 系统	/ 系统配置												
æ	部门		系统配置													
•	用户	~	安全配置	网络配置	HA配置	端口配置	外发配置	认证配置	工单配置	告警配置	审计配置	系统风格				
۲	资源	~	■运维端口	記置										2	编辑	*
•	策略	~														
	运维	~		SSH/SFTP:	22222											
Ĕ	审计	~		FTP:	开启 2121											
Ē	工单	~														
蕶	系统	^	Web控制	的台端口配置										2	编辑	*
				Web控制台端口:	443											
	数据维护			1001201010												
	系统维护		SSH控制	台端口配置										2	编辑	*
	关于系统															
		Ē		SSH控制台端口:	55555											

图 11-16

## 11.5 外发配置

#### 11.5.1 邮件配置

邮件配置用于配置邮件服务器,为报表自动发送功能和账户验证等通知提供邮件发送服务。用户可根据需求设置私有邮箱服务器或是公共邮箱服务器,目前支持两种发送方式— SMTP、Exchange。如图 11-17

III U	CLOUD									⊥ 🗉 Q <sup>12</sup> admin 🗸
-				/ 系統配置		邮件配置		×		
ħ			系统配置			发送方式:	SMTP Exchange			
-		~	安全配置	网络配置	HAā				系统风格	
۲		~	邮件配置			* 服务器地址:	smtp.ucloud.cn 请输入有效的IP地址或域名			∠ 编辑 《
۲		~		发送方式:	SMT	加密方式:	● 无 ○ SSL ○ TLS			
ΩΩ.		~		服务器师师:	smtr	* 端口:	25			
Ú		~		端口:	25		请输入1-65535之间的有效数字			
Ē		~		加密方式:	无	* 发送人账号:	aimee.xue@ucloud.cn			
\$		^		发送人账号:	aime	发送人密码;				
				发送人密码:	****	收件人:				
							发送测试邮件			
			短信配置							∠编辑 ☆
								取消 确定		
		Ē		类型:	内置					

图 11-17

#### 11.5.2 短信配置

短信配置支持两种,一种是堡垒机内置的短信网关,由堡垒机本身的短信网关来提供短信服务;另一种是自定义短信网关,输入正确的 URL 地址和 API 参数后,还可测试所填写服务器信息是否有效。如图 11-18

11 U								⊥ ≣	Q <sup>12</sup> admin	
		桌面 / 系统 / <b>系统配置</b>		短信配置		×				
đ		系统配置		类型:	○ 内置 <b>○</b> webService ○ 自定义					
*		安全配置 网络配置	HA				系统风格			
۲		第二:	25	* 网关类型:	HTTP协议					
ø		加密方式:	无	* 发送方法:	O POST O GET					
ŵ		发送人账号:	aime	★ URL地址:						
Ē		发送人密码:	****	◆ SOAP版本:	SOAP1.1					
Ē				* 编码:						
		短信配置			011-0			2	编辑	
				* 短信模板:	配置短信模板					
		类型:	内置	测试手机号码:						
		SNMP Agent配置			发送测试信息			2		
					E	2消 确定				
		状态:	禁用							

图 11-18

## 11.5.3 SNMP Agent 配置

SNMP Agent 配置分为 V2 和 V3 方式,输入正确的相关信息点击确定(注:类型为 V3 时,认证密码和隐私秘密为必填项),配置完成后用户可以通过 SNMP 客户端或 mac 终端执

第68页共89页

行相关命令获取到堡垒机系统的某些信息 (可以点击 OID 信息表获取相关信息的 OID) 如图

11-19

(1) (1)								⊥ 🗐 Q <sup>122</sup> admin マ
		東面 / 系统 / 系统配置		SNMP Agent配置				
ħ		系统配置		状态:				
*		安全配置 网络配	E HA				系统风格	
۲		加密方	式: 无	类型:	SNMP v3 SNMP v2c			
۵		发送人则	号: aim	* Community:	上座为0.220个空位 带面包会十小空空			
ŵ		发送人图	码: ****		母、数字和特殊字符,不支持空格			
崮		1 45/4 53 B				取消 确定		A 1012 A
B								∠ 蝶稱 ×
۲		3	型: 内置					
		SNMP Agent配置						∠编辑 ☆
			杰: 禁甲					
				UIBER				

图 11-19

## 11.6 认证配置

#### 11.6.1 AD 域认证配置

当企业网络中计算机和用户数量较多时,可实现高效管理。进入 AD 域认证配置页面,点 击添加 AD 域,可选择认证模式和同步模式。填写正确的 AD 域服务器名称,端口,域, Base DN,和登录名密码后,同步方式可选为手动/自动同步。如图 11-20

11 U								⊥ 🗉 Q <sup>12</sup> admin マ
		桌面 / 系统 / <b>系统配置</b>	AD认证配置					
đ		系统配置	* 服务器地址:					
*		安全配置 网络配置 HAT		请输入有效的IP地址或域名		系统风格		
۲		AD认证配置	状态:					+ 添加 《
۷		服务器地址 👻 输入搜索项查询	SSL:					
m		服务器地址 ⇔	模式:	○ 认证模式 ○ 同步模式		步用户数	操作	
Ü			* 端口:	389				
				请输入1-65535之间的有效数字				
•		LDAP认证配置	* 域:					+ 添加 《
		<b>服务器地址 👻</b> 输入搜索项查询		例如: test.com				
		服务器地址 令			取消 确定	作		
				暂无数据	ž			
		RADIUS认证配置						∠ 编辑 《

图 11-20

输入正确参数点击下一步可选择导入源,选择完成后即可导入。如图 11-21

	桌面	桌面 / 系统 / 系统配置	AD认证配置 ×
		系统配置	
		安全配置 网络配置	号入選 ✓ 協入提案項目均 ○.
		服务器地址 - 输入探索项目	- 导入道
_		HERE AS SHARES A	v DC+surfiter,DC+som
		A20070 Q-C-4	Computers
		192.168.40.147	□ ▼ Domain Controllers
			☑ BobFamily
			tuo
		RADIUS认证配置	Out0
			🗹 ou100
		状态:	00101
		服务器地址:	取消 上一歩 構定
		MC1:	812
		认证协议:	AP
		认证共享密钥:	****
		认证相时:	
		86/11/47:	¥ IA

图 11-21

注:

域认证模式是指新建用户时认证类型为 AD 域认证,使用域服务器进行认证机制。 域同步模式是直接同步域服务器上的用户到堡垒机,然后进行认证。

#### 11.6.2 RADIUS 认证配置

按照第三方 RADIUS 服务器的配置信息在 RADIUS 服务器设置页面填写正确的 IP 、端口、 共享秘钥等信息,并可对 RADIUS 用户进行有效性测试。如图 11-22

图 11-22

#### 11.6.3 LDAP 认证配置

云堡垒还支持 LDAP 认证。进入 LDAP 认证配置页面,点击添加 LDAP 服务器,填写正确的 LDAP 服务器地址,端口,OU,选择过滤器类型,点击确定可添加。如图 11-23
(ii) U	CLOUD							⊥ 🗉 Q <sup>12</sup> admin -
-			桌面 / 系统 / <b>系统配置</b>	LDAP认证配置		$\times$		
ħ			系统配置	* 服务器做计:	· 清恤 〉 昭 条 與 他 由			
			安全配置 网络配置 HA		请输入有效的IP地址或域名		系统风格	
۲			LDAP认证配置	状态:				+ 添加 《
۲			服务器地址 ☞ 输入搜索项查询	SSL:				
m			服务器地址 令	* 端口:	389		作	
1					请输入1-65535之间的有效数字			
Đ				* 用户OU:	请输入用户OU			
\$			RADIUS认证配置	* 用户过滤器:	cn 🔍			∠编辑 ※
			状态: 蔡用			取消 确定		
			服务器地址: -					
			第日: 1812					
			认证协议: PAP					
		Ξ	认证共享密钥: ****	**				

图 11-23

## 11.6.4 CAS 配置

第三方 CAS 服务器配置信息在 CAS 配置点编辑,状态开启,填写正确的 CAS 登录服务地址, CAS 服务器部署地址, redirect\_url 等信息。如图 11-24

(iii) U			_				<u>↓</u> 🗏	Q <sup>12</sup> admin 👻
-		桌面 / 系统 / <b>系统配置</b>	CAS配置					
ħ		系统配置	***	:				
<u>.</u>		安全配置 网络配置	HAB CASIR& Bath	. https://boot.port		系统风格		
۲		认证协议:	PAP	nups.most.port				
۲		认证共享密钥:	* CAS服务器部署地址	https://host:port				
Ω.		认证超时:	6 * redirect_u	: https://106.75.134.203:443				
Ë		部门认证:	关闭					
B				取消	确定			
<b>\$</b>		OIDC配置					1	∠编辑 ≪
		17.5	林田					
		(CAS配置					1	≤ 编辑 ◇
		状态:	禁用					

图 11-24

# 11.7 工单配置

## 11.7.1 基本模式

基本模式中可配置访问授权工单申请时的申请范围和命令授权工单的提交方式。如图 11-

25 **A**<sup>12</sup> 桌面 / 系统 / 系统配置 基本模式 系统配置 访问授权工单申请范围: 本部门 本部门及下级部门 • 全部 设置申请访问授权工单时,能够查看到的资源范围 安全配置 网络配置 系统风格 命令授权工单提交方式: 〇 手动提交 〇 自动提交 基本模式 取消 命令授权工单提交方式 高級模式 用户池 用户池 共1条 20条/页 👻 🤇 1 > 前往 1 页

图 11-25

# 11.7.2 高级模式

高级模式中可配置指定部门的用户、角色可以申请指定部门的资源。为用户池和资源池添 加用户所属部门和资源所属部门。如图 11-26

CI U	CLOUD				⊥ 🗐 Q <sup>12</sup> admin 🚽
Ŧ	桌面		桌面 / 系统 / <b>系统配置</b>		
μ.	部门		系统配置		
Ŧ	用户	~	安全配置 网络配置 HA配置 端口配置 外发配置	认证配置 工单配置 告警配置 审计配置	系统风格
۲	资源	~	高级模式		+ 添加 《
•	策略	~	用户池 🔻 输入搜索项查询 🔍		
ŵ	运维	~	用户池	资源池	操作
Ü	审计	~	電気 赤	·市.总部	編輯 删除
Ē	工单	~	-		
蕶	系统	^			共1条 20条/页 🔍 🧹 1 🔀 前往 1 页
			审批流程		∠ 编辑 《
	数据维护				
	系统维护		审批流程: 圖定流程		
	关于系统		审批形式: 多人审批		
		_	审批节点: 用户所属部门-all		
		É	終审节点: 禁用		

#### 11.7.3 审批流程

审批流程设置为分级流程时,系统将自动按照指定的审批节点设置到指定的所属部门寻找 对应的角色用户作为节点,设置为固定流程时,则按照配置寻找节点用户,上限添加 5 个用 户。审批形式设置为多人审批时,每级仅需一个节点进行批准就能通过审批。设置为会签审批 时,则需要同一级的所有节点都批准了工单,工单才能进入下一级审批。审批节点由两部分属 性决定,分别为部门属性和角色属性,部门属性固定有用户所属部门和资源所属部门,角色需 要有管理权限和工单审批权限,只要在指定的部门里的指定角色的用户会自动成为审批节点, 如果用户或资源所在的部门没有对应角色的用户,则自动往上级部门寻找,直到找到总部为 止。审批级数指的是通过工单需要的最大次数,设置为1时,则需要一个节点进行审批,如果 开启了终审,则还需要 admin 用户进行一次审批,级数仅在分级流程时开启,如工单无节点, 那么无论有没有开启终审,都由 admin 审批。如图 11-27

111 UC	CLOUD					⊥ 🗉 Q <sup>12</sup> admin マ
			桌面 / 系统 / <b>系统配置</b>	审批流程		
'n			系统配置	* 审批流程:	○ 分级流程	
-			安全配置 网络配置 HA		按照审批级数逐级进行审批	系统风格
۲			用户池 💌 输入搜索项查询		◎ 固定流程	
۲			用户池		按照固定审批节点进行审批	操作
Ψ			止 总部 	* 审批形式:	○ 多人审批 任意一人批准,则审批通过;任意一人驳回,则审批不通过	编辑 副除
Ë					○ 会签审批	
B					所有人批准,则审批通过:任意一人驳回,则审批不通过	共1条 20条页 👻 🤇 1 🔌 前往 1 页
۰		^	审批流程	* 审批节点:	用户所属部门 👻 all 👻 🚦	∠ 编辑 《
				* 终审节点:		
			审批流程: 圖:		开启终审节点,则需要系统管理员进行最终审批	
			审批形式: 多.		国語	
			审批节点: 用)	_	word HEXC	
		≡	终审节点: 禁用	Ħ		

# 11.8 告警配置

## 11.8.1 告警方式配置

告警方式配置可以修改系统消息、业务消息、任务消息、命令告警、工单消息各级别消息 是否告警和告警方式,包括消息中心、邮件通知、短信通知,默认低级消息不告警;中级消息 告警,只记录消息中心;高级消息告警,记录消息中心和发送邮件。如图 11-28

								⊥ 🗐 🖓admin マ
-		桌面 / 系统 / <b>系统</b>	告警方式配置				×	
		系统配置	消息类型	告警等级	告警	告警方式		
		安全配置 网络	系统消息	低	() 否	前息中心 邮件通知 短	信通知	
		告警方式配置	系统消息	ф	是	☑ 消息中心 🗌 邮件通知 📃 短	信通知	∠编辑 ≪
			系统消息	高	是	🗹 消息中心 🗌 邮件通知 📃 短	信通知	
		消息类型	业务消息	低	() 否	前息中心 🛑 邮件通知 📄 短	信通知	
Ψ		系统消息	业务消息	ф	是	💙 消息中心 🗌 邮件通知 📃 短	信通知	
		系统消息	业务消息	高	● 是	🗹 消息中心 🗌 邮件通知 📃 短	信通知	
		系统消息	任务消息	低	(四) 否	前息中心 的件通知 短短	信通知	
		业务消息	任务消息	ф	● 是	☑ 消息中心 🗌 邮件通知 📃 短	信通知	
		业务消息	任务消息	商	● 是	☑ 消息中心 🗌 邮件通知 📃 短	信通知	
		业务消息	命令告警	低	是	☑ 消息中心 🗌 邮件通知 📃 短	信通知	
		任务消息	命令告讐	中	西 否	前息中心 的件通知 短短	信通知	
		任务消息				Į	消 确定	
		任务消息		高	是	消息中心		
		命令告警		低	授	消息中心		
	÷	命令告警		ф	д	无告警方	πt.	

图 11-28

# 11.8.2 告警等级配置

(iii) U (iii)	CLOUD					⊥ 🗐 A <sup>12</sup> admin マ
-			桌面 / 系统 / <b>系统</b>	告警等级配置		×
æ			系统配置	系统性能 登录 部门 用户	资源 策略 运维	审计 工单 系统
*			安全配置 网络	事件	消息类型	告警等级
۲			工单消息	CPU使用率超过90%	系统消息	○ 低 ○ 中 ○ 商
۲				CPU使用率超过75%	系统消息	○ 低
ŵ			告警等级配置	CPU使用率超过50%	系统消息	● 低 ○ 中 ○ 高
Ë				内存使用率超过90%	系统消息	○ 低 ○ 中 ○ 高
			模块 💌	内存使用率超过80%	系统消息	○ 低
B	工单		系统性能	内存使用率超过60%	系统消息	◎ 低 ○ 中 ○ 高
<b>\$</b>			系统性能	磁盘使用率超过90%	系统消息	○ 低 ○ 中 ○ 高
			系统性能	磁盘使用率超过80%	系统消息	○ 低
			系统性能	磁盘使用率超过75%	系统消息	● 低 ○ 中 ○ 高
			系统性能	备节点宕机	系統消息	○ 低 ○ 中 ○ 高
			系统性能			
			系统性能	141	2014 CO 100	
		Œ	系统性能	ф	系统消息	磁盘使用率超过80%

告警等级配置"可以修改各模块各类型消息的告警级别。如图 11-29

图 11-29

# 11.9 审计配置

进入审计配置可查看到当前 OCR 的状态, 启用 OCR 后可对图形协议进行文字识别。只 对图形协议有效。输入正确的 OCR 地址即可。如图 11-30

							🛓 🗐 🗘 admin 👻
-		桌面 / 系统 / <b>系统配置</b>	OCR配置				
		系统配置	状态:				
		安全配置 网络配置 HA	¥ 服务器地址:			系统风格	
		OCR配置	00000	请输入有效的IP地址或域名			∠编辑 ☆
		状态: 蔡	A		取消 确定		
		服务器地址: -					
		OCR服务状态: -					
	^						

图 11-30

# 11.10 系统风格

⊥ 🗐 🖓 admin 🦷 桌面 / 系统 / 系统配置 - 桌面 **山** 部门 系统配置 安全配置 网络配置 HA配置 端口配置 外发配置 认证配置 工单配置 告警配置 审计配置 系统风格 系统语言: 简体中文 资源 策略 V 图标配置 ∠ 编辑 运维 nh: Ë 88\*28像素的透明底PNG图片 系統图标 Ē 🖽 UCLOUD • 28\*28像素的透明底PNG图片 ГЛ П 数据维护 系统维护 关于系统 图 11-31

进入系统风格后,可更改系统语言,和企业图标。如图 11-31

### 11.11 数据维护-存储配置

# 11.11.1 存储概览

存储概览主要展示当前堡垒机系统的系统分区和数据分区的空间使用量。如图 11-32

11 U					⊥ ≣	Q <sup>12</sup> ad	lmin 👻
-	桌面		桌面 / 系统 / 数据维护				
đ.	部门		数据维护				
Ŧ	用户	~	存储配置 日志备份				
۲	资源	~	存储概览				*
9	策略	~					
Ψ	运维	~	系统分区:	<b>10.3%</b> 22.038可用,共24.5GB			
Ü	审计	~					
È	工单	~	数据分区:	<b>20.5%</b> 32.6GB可用,共41.0GB			
⊘	系统	^					
	系统配置		网盘空间			∠ 编辑	*
	系统维护		个人网盘空间:	500MB			
	关于系统		网盘总空间:	5120MB			
		IJ	自动删除			∠ 编辑	*

图 11-32

## 11.11.2 网盘空间

11 U						⊥ 🗉 Q <sup>122</sup> admin マ
-		桌面 / 系统 / 数据维护	编辑网盘空间			
ф		数据维护				
		系統分区: 1	个人网盘空间: 0.3 <sup>3</sup> 2.0	500 有效值为大于等于0的整数。如果设置为	MB	
۲				C, MPTHENT AMIMAAJ		
۲		数据分区: 2	网盘总空间: 0.5	5120 有效值为大于等于0的整数。如果设置为	MB	
Ψ.			2.0	U, RITHKBIRGMANACI		
É		网盘空间			取消 确定	∠ 编辑 《
Bì						
•		个人网盘空间: 5	00MB			
		网盘总空间: 5	120MB			
		1.000				
		目动删除				∠ 编辑
		自动删除: 非	補			
	Ē	空间满时覆盖之前数据:	3用			

网盘空间可查看更改个人网盘空间和总空间。如图 11-33

图 11-33

# 11.11.3 自动删除

自动删除用户是否开启磁盘自动清除,和空间满是自动覆盖最早的数据,自动删除默认为 删除 180 天前的数据,如 180 天前的数据删除完后磁盘还是无空间,则继续一天一天往前自 动删除。配置如图 11-34

(1) (1)					上 🗏 💭 admin 👻
-		桌面 / 系统 / 数据维护	自动删除		
đ		数据维护	自动删除:		
.≖	~	网盘空间		设置是否启用自动删除功能	∠ 编辑 《
۲	~		空间满时覆盖之前数据:	开启后,当数据分区的剩余空间小于10%或	
۲	~	个人网盘空间: 50	01	者5GB时,会覆盖历史会话,系统日志等 数据。	
œ	~	<u> </u>	20		
Ü	~	自动删除		取消 确定	∠编辑 ☆
B	~				
\$	^	自动删除: 禁	Ħ		
		空间滿时覆盖之前数据: 启,	Ħ		
		手动删除			
		副院 (日期) 前的数据:			
	Ŧ	DIG TELEP BUT DAM			

图 11-34

第77页共89页

# 11.11.4 手动删除

۳u	CLOUD				⊥ 🗉 Q <sup>12</sup> admin –
Ŧ	桌面		桌面 / 系统 / 数据维护		
ф	部门		数据维护		
Ŧ	用户	~	网盘空间		∠编辑 ≪
۲	资源	~			
9	策略	~	个人网盘空间:	500MB	
m	运维	~	网盘总空间:	5120MB	
Ŭ	审计	~	自动删除	(( ( 2001年4日 ) )))	∠ 编辑 ※
	工单	~			
	系统	^	自动删除:	28 29 30 31 <b>1 2 3</b>	
	系统配置		空间满时覆盖之前数据:	4 5 6 7 8 9 10 11 12 13 14 15 16 17	
				18 19 20 21 22 23 24	
	系统维护		手动删除	9天 26 27 28 29 30 1 2 2 4 5 6 7 8	*
	关于系统		删除 (日期) 前的数据:		
		≡			
				图 11-	
				2	
0.00			_	5	1 5 (12)
				Hate Hard Hard Hard Hard Hard Hard Hard Hard	⊥ 🗐 Ļ admin 👻
-			果叫 / 系统 / <b>数据维护</b>		
ŵ			数据维护		

支持手动删除选择日期天前的数据。如图 11-35

Ŧ		桌面 / 系统 / 数据维护	日志本地备份					
đ.		数据维护	<ul> <li>* 日志内容:</li> </ul>	系统登录日志 资源登录日志				
		存储配置 日志备份		□ 命令操作日志 □ 文件操作日志				
۲		本地备份					十 新建	
۲			* 时间范围:	<b></b>				
m			备注:			操作		
崮				描述最长128个汉字或字符				
B		远程备份至syslog服务器					∠ 编辑	
\$			_		取消 确定			
		状态: 禁用						
		备份内容: 系统登录	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				
		远程备份至FTP/SFTP服务器					∠ 编辑	
	Ē	状态: 禁用						

# 11.12 数据维护-日志备份

# 11.12.1 本地备份

进入日志备份,点击本地备份右边的新建,选择要备份的日志内容,和时间范围,点击确 定即可完成备份。如图 11-36

<b>N</b> i	它匣子																		23	<u>+</u> 🗉	000	admin	
			AR / AR / REAP	日志本地备份											1								
rh.			数据维护												1								
2			存储配置 日志备份	日志内容:	<ul> <li>✓ 系統型</li> <li>✓ 命令損</li> </ul>	】录日3 】	5		た源登 て件操	录日志 作日志					I								
۲			本地备份		🗹 双人想	权日常	5								1						+ 168		
0				• 时间范围:	1					C	1									10.00			
Ţ.				备注:	~	<	2019	9年5	5月					201	9年	6月	>	»		-parte-			
8					H	-	1	Ξ		五万	*	B		-	Ξ	23	E	*					
	工单				5	6	7	8	9	10 1	11	2	3	4	5	6	7	8					
			1 延续重加至sysiog融为值		12	13	14	15	今天	17 1	18	9	10	11	12	13	14	15			Z. 01#		
a.			状态:	启用	19 26	20	21 28	22	23	24 2	25	16	17	18	19 26	20	21	22 29					
	赤纸配置					3	4	5	6	7 0		30	1	2	1	4	5	0					
			备份内容	系统登录日志;资源登录日志;命令		-	-		-	-	-			-	-		-	-					
			┃ 远程备份至FTP/SFTP服↓	5월																	之 编辑		
			47121-	6 <b>m</b>																			
			(传输模式+)	SFTP																			
		#	备份内容:	系统配置:会话回放日志																			

# 11.12.2 远程备份至 syslog 服务器

点击编辑配置 syslog 服务器,填写标识后输入正确的 syslog 服务器地址,勾选备份内容 后,当执行了备份内容中的操作时,会自动备份到 syslog 服务器中。配置如图 11-37

L 用户 Y 日期 petrom###現在 推作 推作	
ologitik) illihort	
◆ 资源 ~	
● 策略  ● 策略  ● 度送者标识: FUCK ● 使用したのや第二ののや第二ののや第二ののの第二のののでの	
· 服务器P: 106.75.172.219	
1         0000·································	
新始内容: <b>新</b> 统	
<ul> <li>♦ Asi:</li> <li>• bbik:</li> <li>□ TOP</li> <li>● UDP</li> </ul>	
系統配置 」 远程备份至FTP/SFTP服务器	
x###	
* 爸的内容: ✓ 系统登录日志 系统经验	
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
关于系统 彻临隔底 BFT	
金份內容: 系統	



## 11.12.3 远程备份至 FTP/SFTP 服务器

点击编辑将状态改为开启状态后可选择 FTP/SFTP 服务器,输入正确的参数后可选择备份 内容,支持系统配置和会话回放日志。支持手动备份今天之前的日志到 FTP/SFTP 服务器上。 配置如图 11-38

							⊥ 🗉 🗘 admin 👻
		桌面 / 系统 / 数据维护	远程备份至FTP/SFTP服	场器	×		
		数据维护	状态:	■● 系統每天定时在零点进行前一日的数据备份 (次图日志为实时备份), 启用后会将数据备 (本及运用ETO/CTTD图条例)			
		日期		辺玉島福戸17/371戸腺労会		操作	
			FTP/SFTP服务器配置				
ø			* 传输模式:	O FTP O SFTP			
		┃ 远程备份至syslog服务器	<ul> <li>服务器P:</li> </ul>	10.13.48.217			∠ 编辑 ※
			100 P 3 100				
		状态: 禁用	* 端口:	22			
		备份内容: 系统		〒骊八1−00030之间的有奴奴子			
			* 用户名:	root			
		┃ 远程备份至FTP/SFTP服务器	* 密码:				∠ 编辑 《
		状态: 禁用	存储路径:				
		传输模式: SFTF		测试连通性			
	关于系统	备份内容: 系统					
			* 备份内容:	✔ 系统配置			

图 11-38

# 11.13 系统维护-系统状态

进入系统状态可查看 CPU/内存使用率,磁盘读写状态和网络收发状态,点击可展开。如 图 11-39

🖾 υсιουσ	⊥ ≣ ג <sup>10</sup> admin ~
重 桌面	桌面 / 系统 / 系统维护
▲ 部门	系统维护
上 用户 ~	系统状态 系统管理 配置备份与还原 授奴许可 网络诊断 系统诊断
	CPU/内存使用率 余
	5分钟 15分钟 10时
- 空 运维 イン	
曽 审计 ~	◆ CPU ◇ 防存
■ 工单 ~	
	80%
系统配置	
数据维护	40%
系统维护	20%
关于系统	0%
≡	

图 11-39

## 11.14 系统维护-系统管理

进入系统管理可查看到当前系统地址,系统时间(输入正确的时间服务器地址可同步时 间),系统升级(点击升级后上传正确的升级包,点击确认升级,系统即可自动升级),系统 工具(具有重启,关机和恢复出厂设置功能)。如图 11-40

10 III			$\downarrow$	Q <sup>12</sup> admin 🔻
-	桌面		桌面 / 系统 / 系统维护	
đ	部门		系统维护	
•	用户	~	系统状态 系统管理 配置备份与还原 授权许可 网络诊断 系统诊断	
۲	资源	~	系统地址	*
9	策略	~		
Ψ	运维	~	系统地址: 106.75.175.26 立即更新 当系统位于NAT或防火墙后,请设置为	
Ü	审计	~	NAT外网地址。否则会导致FTP等应用无法 连接	
Ē	工単	~		
ଡ଼	系统	^	系統时间	*
	系统配置		当前时间: 2021-04-25 17:44:21 Sunday 傅改	
	数据维护			
			时间服务器: cn.ntp.org.cn 同步时间	
	关于系统		T de La	
			_ 4%\$UT 5X	*
		≣		

图 11-40

# 11.15 系统维护-配置备份与还原

#### 11.15.1 备份列表

点击新建, 弹出确认备份弹窗, 可以输入备注信息来区分备份文件, 点击备份开始备份, 备份成功后, 页面提示系统配置备份成功。可将备份文件下载到本地。打开自动备份按钮后, 系统将在每天零点自动进行配置备份。如图 11-41

(iii) U										⊥ 国 🖓 🔁 admin 👻
	桌面		桌面 / 系统 ,	/ 系统维护						
.th	部门		系统维护							
•	用户	~	系统状态	系统管理	配置备份与还原	授权许可	网络诊断	系统诊断		
۲	资源	~	备份列表							○ 自动备份 + 新建 ☆
9	策略	~	日期			版本		文件大小	备注	操作
ŵ	运维	~						暂无数	IE .	
Ŭ	审计	~								
Ē	工单	~	配置还原							*
蕶	系统	^								
	系統配置			上传文件:	点击上传	14讲行配置条份	并确保上传的新	语文化完整		
	数据维护									
	关于系统									
		E								

图 11-41

# 11.15.2 配置还原

点击上传文件后,上传备份文件即可看到弹窗:是否还原配置,点击确定后可还原。如图 11-42

	桌面		桌面 / 系统 / <b>系统维护</b>				
ф			系统维护				
		~	系统状态 系统管理	配置备份与还原 授权许可 网络诊断	系统诊断		
۲		~	备份列表				○ 目动备份 +新建 ↔
۲	策略	~	日期	版本	文件大小	备注	操作
w		~	2019-05-15 04:58:48	确认	×	test	还原 下载 删除
١.		~					
в		~		稳定要还原系统配置?			20条/页 👻 🤇 1 ) 前往 1 页
۲		^	配置还原		取消 确定		*
	系统配置						
	数据维护		上传文件:	点击上传			
				请在还原系统配置前先进行配置备份,并确保上传的部 ② backup-20190515045848.bak	2置文件完整		
	关于系统						
		≡					

# 11.16 系统维护-授权许可

点击更新许可证,弹出弹窗,点击下载,下载许可申请文件,发送给售后人员,由售后人员生成授权文件,点击上传,上传售后人员发来的授权文件,完成更新授权。如图 11-43

				<u> </u>	admin 👻
Ŧ			桌面 / 系统 / <b>系统维护</b>	更新授权 ×	
			系统维护	申请许可: 下载	
		~	系统状态 系统管理	配置 下盤许可申请文件,并联系供应商申请授权许可	
		~		导入许可文件: 点击上传	
		~	授权信息:	udo	
		~	授权类型:	正式 取消 确定	
		~	状态:	已激活 更新许可证 备份许可证	
		~	产品ID:	df06b433757142bfb8c1d70a0bca7585	
		~	授权模块:	基础模块,自动化运维,数据库审计,OCR,APP	
			授权资源数:	20	
			授权资源并发连接数:	40	
			过期时间:	2021-12-24 09:56:32	
	关于系统				
		Ē			

图 11-43

# 11.17 系统维护-网络诊断

进入网络诊断后, 连通性测试可以执行 ping、路由追踪、TCP 端口检测操作, 输入正确 格式的 IP 地址和端口, 点击执行, 会有结果信息显示。如图 11-44

13 U				↓ E	Q <sup>12</sup> admin -
-	桌面		桌面 / 系统 / <b>系统推护</b>		
đ.	部门		系统维护		
-	用户	~	系统状态 系统管理 配置备份与还原 授权许可 网络诊断 系统诊断		
۲	资源	~	连通性测试		*
٢	策略	~			
Ψ.	运维	~	信息类型: Oping OB由追踪 OTCP端口检测		
Ë	审计	~	主机地址: 10.142.12.45		
Ē	Т¥	~	编辑人IP44地址,点分于近初推式		
蕶	系统	^	PING 10.142.12.45 (10.142.12.45) 56(84) bytes of deta.		
	系统配置		10.44.12.49 pmg stanstos 4 packets transmitted, 0 received, 100% packet loss, time 2999ms		
	数据维护				
	关于系统				
		≡			

图 11-44

# 11.18 系统维护-系统诊断

进入系统诊断后,可选择信息类型获取信息。如图 11-45

[]] U			<u>↓</u>	Ξ	Q <sup>12</sup> admin 👻
-	桌面	桌面 / 系统 / 系统编护			
ф.	部门	系统维护			
•	用户	系统状态 系统管理 配置备份与还原 授权许可 网络诊断 系统诊断			
۲	资源	_			
	策略	信息类型: 综合信息 承 获取信息			
ŵ	运维	综合信息 ory			
Ű	审计	cache si so bi bo in cs us sy idi wa st 的存信息 1522280 0 0 0 15 0 2 0 99 0 0			
Ē	工单	网卡信息			
蕶	系统	和風にからる			
	系统配置	ARP信息			
	数据维护				
	关于系统				

图 11-45

#### 11.19 关于系统

进入系统-关于系统可查看当前系统相关内容。如图 11-46

C U				⊥ E 0 <sup>10</sup> admin ~
	桌面		桌面 / 系统 / 关于系统	
đ.	部门		关于系统	
⊻	用户	~		
۲	资源	~	产品名称:	堡垒机
۲	策略	~	产品ID:	df06b433757142bfb8c1d70a0bca7586
Ψ.	运维	~	服务码:	童筍
Ë	审计	~	API凭证:	待更新 更新 堂書 清除
Bì	工单	~	HA Key:	更新于 2019-07-08 16:13:50 更新 查看
蕶	系统	^	版本号:	V1.0
	系统配置		设备系统:	V3.4.8.0
	数据维护		发行日期:	2020-09-01
	系统维护			Copyright © 2012-2019 UCloud
	关于系统			
		E		

图 11-46

## 12 附录

## 12.1 应用发布服务安装配置

应用发布服务器要完成自动代填,需要进行配置才可以;以下附上配置方法:

### 12.1.1 安装 RemoteApp 跳板程序

(前提需要微软的.Net 框架),程序请向售后人员等索要;

#### 12.1.2 配置 FireFox

配置 FireFox; 首先安装 FireFox, 然后在命令行中执行命令 "FireFox 安 装目录\firefox.exe" -no-remote -p default, 执行完命令后会启动 Firefox 浏览 器,这时候找到"附加组件-扩展-从文件中安装附加组件"将插件(该插件 由售后人员提供)安装到浏览器,

)火狐主页,教御使用 Firef	×/ * PEDBHYBTEH × (+				
Forto: aboutaddons	C Q Age vChicks	2	1 0 4 1	9 h -	t 📑
最常选问 🧾 火氣會方站也 🗌	新手上路 🣴 常用同论 🛄 紙用室		× 1941	11. 89	0 886
		0.	-	100%	+
E REALIZATION (*				00	
17展	标签页优化 公園17月14時に半月6日半約数以行为、万学専用、 単多		和政治口	新聞的私の問題	(1)(9)[7][10]
in 19. 10	■ 附价组件管理器			0	<d></d>
Julian, marken front. Drafter Aboutationer Barken Julian Status Barken Julian Status Practice Status P	Reference Refere			历史记录	全罪
		ardania noriena. 🛤	Q	0	*
	* 火爆主页 火爆主性型、生活物运动可测、希望或可加30.28所是为# 第5		يو	8	
	一 网页截图 方带的此时工具、方叶任常治定后线更高、全共可能图解4件截图方式、并微约心带的图计编码功能。更5		开发者	火箭停架工具	
	网根支付助手 http:///www.marketing		C BRORD		0 0
	▲ 西南市市市市大学研究社会 Findex 4 (21)1、通道的目前。 7 (61)11(1) ●		usu (	熱用	8H
	▲ yuz firefox 4總防從兵 Firefox 十段用,清澄始起用。 7%121				1710
	a basic add-on of yurwiad \min			and a	
	添加xpi插件				
		100/15 W 時到"世界	/indows I圓板 中的 系统	UIIIS Wind	
为提高用户体验,Firefox 将发行	这部分功能的根用整份和我们,用于进一步统化火集团后期的基用性,您可以同时也是是是内的们分享数据。			這样切樂方	

拖放并安装好插件后, 打开

C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles,检查是 否存在一个\*.default的文件夹,并将该文件夹下的内容拷贝到 C:\DevOpsTools\RemoteAPPProxy\Browser\Firefox\fc4fa298.default 替换 (先将 fc4fa298.default 目录下文件清空再粘贴),在目录 C:\DevOpsTools 下创建文件夹 Firefox,文件夹包含文件有 firefox.bat、 firefox.exe、firefox.vbs、md5.vbs(请向售后人员等索要),确保 vbs 脚 本编码格式是 ANSI,通过另存为可以看到编码格式,如果是其他编码 格式请修改为 ANSI 格式保存

#### 12.1.3 配置 Chrome

配置 Chrome, 与 FireFox 类似, 首先安装 Chrome, 在 cmd 命令行执 行 start chrome.exe --user-data-dir=C:\User\chromeaccounts\default, 执行 完命令后会打开 Chrome 浏览器, 打开拓展程序安装界面,拖拽代填插件 chrome.crx 插件 (售后人员提供) 到 chrome 浏览器中进行安装, 然后到 文件目录 C:\User\chromeaccounts 查看是否有 default 文件夹, 并将 default 文件夹下的内容拷贝到

C:\DevOpsTools\RemoteAPPProxy\Browser\Chrome\Default 替换,在目录 C:\DevOpsTools下创建文件夹 Chrome,文件夹包含文件有 chrome.bat、chrome.exe、chrome.vbs(请向售后人员等索要),确保 vbs脚本编码格式是 ANSI,通过另存为可以看到编码格式,如果是其他 编码格式请修改为 ANSI 格式保存