

数据融合与安全专家

深圳云安宝科技有限公司

文档版本: V3.2.8.0

2018年12月27日



目录

1.	信息	完善与帐号创建
	1.1.	完善管理员信息3
	1.2.	创建堡垒机用户帐号4
2.	资源:	录入5
	2.1.	添加主机5
	2.2.	添加资源主机帐号9
		2.2.1. 手动登录帐号
		2.2.2. 自动登录帐号10
		2.2.3. 提权登录11
3.	授权.	
	3.1.	访问策略11



前言

云匣子_堡垒机是租户连接云资源的安全管理工具,帮助云租户更加安全、 精细的管理云上的虚拟机、数据库等资源。

1. 信息完善与帐号创建

1.1. 完善管理员信息

首次以 admin 帐号登录,在页面右上角,点击帐号右边的下拉按钮,进入 [个人中心/编辑],显示当前个人帐号信息,在页面中可以编辑,如图 1-1-1、1-1-2 所示。



्र च	17												□ 0 ³⁰ admin	-
	155 N)		5 用 ^曲	2	4 ±லி) 定用	9	0 应用服务器			1 告望	三 个人中心 三 適出	Ļ
	Þ	~	▲ 活动用户		1	6 侍审批工单			0	主机类型统计				L
• a	1277	~	admin sys-admin		192.168.13.1 2018-06-01 15:01:24									L
9 9	inti	~										SSH		L
w z	54 0	~					智无数据					RDP		L
i i	ù†	~												L
B I	ļφ.	~												L
♥ 5	i#5	~	◎ 应用美型统计			2 当前活动会话				▲ 今日新增会适				I
							0 1				2 会话歌	461.6KB 会运大小		
				智无数据		字符			0	学符			2/461.6KB	
						開売			O	图形			0/0B	
						文件传输			0	文件传输			0/0B	
			- 登录次数统计		本周本月	🛄 這線次跟給计		本度	本月	▲ 這應用 ^A Top5			本問 本月	
			3			2			,	admin sys-admin			2	
		≡			/			/	/					v

图 1-1-1

) te:	7				E 🖓 admin 👻
		allin / 个人中心	编辑个人信息	×	
∰ #		个人中心	. 167	an admin	
▶ 用户		个人中心 手机令牌 SSH公钥 我	的权限 我的日志	555-5000000 长度1-12个汉字成字符,允许输入汉字、 字母、翰字、"母"、"云"、"宝"、	
<u>ب</u>		基本信息	• 手机:	1890000000	∠ अक्ष
9 #88		登录名: admin		手机号十分重要,请输入有效的中国大陆手 机号码	
₩ 201		图码: ****** 修改密码	• d##1 :		
i #3		姓名: sys-admin			
B IA		手机: 1890000000		RGH MAGE	
🗢 35.6		ADAN : -			
		角色: 系統管理员			
		18(1): 218			

图 1-1- 2

1.2. 创建堡垒机用户帐号

进入到[用户/用户管理]菜单栏,点击页面右边的"新建",其中"*"标记 的红色部分为必填项,登录名、密码、姓名、手机、邮箱、请参考页面上提示 信息进行填写,角色和部门以及认证类型根据实际情况进行选择。如图 1-2-1 所示。



N :	三匣子										🗉 🔎 🕮 admin 👻
				用户 / 用户管理		新建用户					
đ			用户	管理		• 登录名:	test		^		C 32 🛤
<u>.</u>			25	2名 マ 編入授業項書店	() 高級撤索		1:1=,+?~@				9 41
ſ		٦		聖荣名 ⇔	ES.	* 密码 :	•••••			\$10 V	援作
				zhangsan	жΞ	 總认密码: 	•••••			22	管理 加入組 删除
				wangmiao	王章		随机生成 夏朝密朝 长度为8-32个字符,需要包含大小写字 母 新学时转动学校,工艺技巧体			95	管理加入组织中
				lýti	\$2:H		201 3012-041036-0110-2-0120-0012-041			研发部	1998 加入組 開始
				lsi	李四	• 姓名:	测试 长度为1-12个汉字或字符,允许输入汉			研发部	管理加入组织的
				admin	sys-a		字、字母、数字、1@1、17、127成14			总部	管理 加入组
						• 手机:	1366666666				
m							于机号十分重要,谓输入正确的于机号码				
Ü						• 664G :	ceshi@yunanbao.com.cn				
в						* 角色:	运搬员 🔻				
						 Mineral J: 	9 8 •		×		
								Riji Rij			
											20 余页 👻 🤇 1 🔿 前往 1 页

图 1-2-1

2. 资源录入

2.1. 添加主机

进入到[资源/主机管理]菜单栏,录入主机信息分为单个录入与批量添加, 批量添加又存在2种方法:一种为本地表格模版导入,另一种从云平台导入 (适用于云主机)。

单台主机录入,点击页面右边的"新建"如图 2-1-1 所示。



N :	三匣子										🗉 🗘 🕮 admin	Ŧ
			() 読返 /	主机整理		新建主机			×			
m		Э	E机管理						^		S \$2	J
			主机名称		20080	 主机名称: 	CentOS6.5 长度为1-64个汉字或字符,允许输入汉				83	
				20. *	±#1986 *		字、字母、数字、***域**			90 T	11/1	
	主机管理			CentOS-6.5	192.168.13.123.2	• 协议典型:	SSH 🔻		-	総部	管理 更多	
	的田田水			Wn-7	192.168.13.100:3	 主机地址: 	192.168.66.66			8	警理 更多	
				CentOS-13.123	192.168.13.123.2		请输入有效的IP地址或域名			.0#	110 R.S.	
				RetHat-38	192.168.13.138:2	• 90E3 :	22 演输入1.65535之间的有效数定			研发部	管理 更多	
-												
						3.69.22 :	Linux 👻					
ŭ						更多匹呗:	☑ 文件管理 ☑ RDP参切报					
						• (#FREERVT) :	研发部 👻					
B						5.00 ·	-					
•						Print 1	输入完毕后,回车自动创建新标签		~			
								Rifi T-#	2			
											20 条页 👻 < 🕇 🔿 載柱 🚹 页	

图 2-1-1

单台录入设备时,会提示,是否需要立即添加该资源主机上的系统帐号。如图 2-1-2 所示,如若需要添加,按照提示填写即可,否则选择"以后添加"



新建主机		×
添加账户:	○ 立即添加 ○ 以后添加	^
* 登录方式:	自动登录	
* 主机账户:	□ 特权账户	
* 密码:		
SSH Key :		
	填写之后将优先通过SSH Key登录	
passphrase :		
账户描述:		
	描述最长128个汉字或字符	~
	取消上一步	确定

图 2-1- 2

本地模版导入则点击页面右边的"导入",提示需要下载模版,点击下载,模版 如图 2-1-3-1、2-1-3-2 所示



	A	В	с	D	Е	F	G	Н	I	J	K	L	М	Ν	0	Р	Q	E
1	名称(IP地址/域名	协议类型	端口	系统类型	所属部门(标签	主机描述	主机账户	登录方式(自动登录	特权账户(;	密码	SSH Key (S	Spassphrase	切换自(输	切换命令	账户描述	(描:
2	主机1	1.1.1.1	SSH	22	Cisco	总部,部门	1		root	自动登录	是	password						
3																		
4																		
5																		
6																		
7																		
8																		
9																		
11																		
10																		
12																		
14																		
15																		
16																		
17																		
18																		
19																		
20																		
21																		
22																		
23																		
24																		
25																		
26																		
27																		
28																		
29																		
30																		
-31	÷.	工作表1	(†)							i 4								•





图 2-1- 3-2

直接从云上导入主机,如图 2-1-4 所示。



) र	三匣子									E 4 ⁶	admin 👻
		- 1		1 / 主机設理		导入主机					
			主机管	理						C \$2	新建
		~	主机名	8 输入物变现变法	 () () () () () () () () () () () () () (导入方式:	○ 从文件导入 💽 导入云主机				8:1
					-	 云平台: 	○ 阿里云 ○ 百度云 ○ 华为云			100 Au-	
				GentOS-6.5	±01788E ≑		○ 廣讯云 ○ AWS ○ Azure		201	501- 103	重文
				Wn-7	192 168 13 100 3		ODCloud		522	104 107	TS .
				CentOS-13.123	192.168.13.123.2	 Access Key ID : 		0	0.00	53	更多
				RetHat-38	192.168.13.138.2	Access Key Secret :			研发部	管理	更多
						优先导入IP:	○ 公園 ○ 内岡				
		×					_				
		~				更多选项:	教養已有主机 教養已有主机				
		~						Riti			
		~									
		\sim									
		=							20 条/页		1页

图 2-1-4

2.2. 添加资源主机帐号

2.2.1. 手动登录帐号

进入到[资源/资源帐号]菜单,点击页面右边的"新建",出现编辑框,拉选 登录方式为"手动登录",关联相关的资源主机即可。需要注意的是,此时,资 源账户这一栏并不是必填项,如果不填,添加的帐号为"Empty",即手动登 录,访问资源时需要手动输入账户名和密码。如果填写了资源帐号,添加的帐 号为填写的帐号,访问资源时需要输入对应系统帐号的密码。



	己匣子											Ξ	Û	dmin 🔻
			22 / 223 900		新建账户									
đ		資源则	KP					^				3	× [ist.
		121099	KP - 编入搜索项查询		* 关联资源:	诸法释关款资源	-							\$ 33
			8386 ¹	*1227	登录方式:	手动型录	•		日本方式 マ	部(1) 🔻		10.75		
			(Empty)	CentOS-6	155209967 ⁴⁴ :				手动登录	总部		10 H H	λia a	
			(Empty)	Wn-7					手动登录	总部		管理 加	入组	
	202200000000		(Empty)	RetHal-38	30 333:				手动登录	研发部		管理 加	入網	19
	Bilderer		test	CentOS-6.	SSH Key :				自动登录	88		管理 加	Хя I	1 10
			root	CentOS-13					自动登录	.089		智理加	入組	19 2
			root	RetHat-38		填写之后将优先遣过SSH Key登录			自动登录	研发部		管理 加	λie i	898
m			administrator	Wn-7	passphrase :				自动整荣	9 3		管理加	入组	194
Ü					contramo a									
В					96/*986 <u>8</u> :									
						据述最长128个汉字或字符								
							Beiter and							
							400 900							
											20 劉页 🔻	< 1 >	前往	1 页

图 2-2-1

2.2.2. 自动登录帐号

自动登录帐号,其实就是已经把密码托管给了堡垒机的资源主机系统帐 号,因此在访问资源主机时,堡垒机会将管理员托管进去的密码自动发给对应 的资源主机,以实现无需人工手动输入密码的过程。

选择登录方式为"自动登录",关联对应的资源主机,填写需要托管密码的 系统帐号,然后将该帐号的密码托管给堡垒机,如图 2-2-2 所示。

	己匣子											E 0	admin 👻
			/ Home / Homeson		新建账户								
di.		资	陳账户					^				0 \$X	新聞
			contracts and a single first		• 关联资源:	SSH@Cent0S-6.5@192.168.13.1							84
				Heretalar	登录方式:	自动要荣							
-			资源账户 ≑	关联资源					登录方式 ▼	部门 👻		提作	
			[Empty]	CentOS-6.	• 3539967** :	root			手动登录	总部		管理 加入組	***
			[Empty]	Win-7		✓ 特权账户			手动登录	心部		管理 加入组	創除
			[Empty]	RetHat-38	• 18595 :	•••••			手动登录	研发部		管理 加入組	35 59:
			test	CentOS-6.					自动登录	总部		管理加入组	豊珍
			root	CentOS-12	SSH Key :				自动登录	101 111 111		管理 加入组	潮 除
۲			root	RetHal-38					自动登录	研設部		管理 加入組	
Ω.			administrator	Wn-7		填写之后将优先遭过SSH Key登录			自动登录	25		管理 加入组	創除
Ű					passphrase :								
					967*1962E :			-					
						据试展长128个项型成型的		~					
							107166 20000						
							-6079						
											20 条/页 🔻	< 1 > 前	主 1 页

图 2-2- 2



2.2.3. 提权登录

提权登录的概念为,当一个普通用户登录到目标资源主机上时,进行一次身份 切换,登录到特权帐号。选择该方式时,需要先填写特权帐号密码,然后选取 做切换的普通帐号。如图 2-2-3 所示。

N ;												e 4	admin 👻
			22 / 252064		新建账户								
da		资源则	(P					^			C	\$ λ	标准
		2010000			• 关联资源:	SSH@CentOS-6.5@192.168.13.1 V							84
					登录方式:	提权要荣							
*			例 测频 /**	关联资源				3	2最方式 ▼	部(1) 👻	1		
			[Empty]	CentOS-6:	125209967 ⁴ 4 :				戶动發展	总部	t	融 加入組	新 绘
			(Empty)	Wn-7		✓ 特权账户		÷	戶助登录	9 %	8	理 加入组	新玲
			(Empty)	RetHat-38	• 密码:	•••••		-	戶动登录	研发部	,	理 加入組	無除
			lest	CentOS-6				1	的登录	总部	t	理 加入组	業体
			root	CentOS-13	SSH Key :			E	目动登录	总部	1	躍 加入組	** *
۲			root	RetHat-38				1	自动登录	研发部	1	國 加入組	# \$\$
m			administrator	Wn-7		填写之后将优先遣过SSH Key登录		E	自动登录	.e#	1	理 加入组	業除
Ë					passphrase :								
B					• 切錄自:	请选择资源账户 >							
						请选择从哪个账户切换为该账户							
					▲ PHSE.d.A.			Ť					
							Riji Nii						
	=										20 条/页 👻 🤇	前社	1页

图 2-2- 3

3. 授权

3.1. 访问策略

在创建完堡垒机用户以及将服务器资源信息纳入堡垒机之后,需要创建一条策略将对应的堡垒机用户与对应的资源主机进行关联起来。进入[策略/访问 控制策略],如图 3-1-1 所示,可以查看备份记录列表。



	三甲子					E 4	admin 👻
Ĩ			夏雨 / 節略 / 透明波制築略	新建访问控制策略	×		
Ē			访问控制策略		^	CO	and a
h				* 策略名称:			_
*			第略名称 ▼ 輸入建築現金調 Q		长度1-64个汉字成字符,允许输入英文字母、数字、成""		製出
٠			□ 策略名称	* ##20208 :	the C RiteXLE		
۲			日 研发1组专用	• 文件传输:	v)@RetHat38 智徳	关联更多	# \$\$
	访问控制领暗]					_
				更多进项:	☑ 文件管理	大款 更多	
			Linux	登录时段限制:		关联 更多	
m							
Ľ			列車按照优先级从海到低非序,支持拖动改变优先级顺序				
_					0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23		
•				IP限制:	#84 V		
					~		
					R036 T		
					20 级页 🔍 🔍	1 〉 就	[1页]

图 3-1-1

编辑创建[访问策略]对话框,先输入一个名称,然后可以设置该访问策略的 有效期与生效时间,有效期不设置时为一直生效。限制文件的上传、下载以及 文件管理、RDP 剪切板等功能,然后点击下一步,去关联对应的堡垒机用户和 相关的资源主机与账户,支持直接关联组。如图 3-1-2-1 和 3-1-2-2 所示。



新建访问控制策略			\times
关联用户 关联用户组			
			7
可选择的用户		已选择的用户	
请 輸入关键词查询 Q		请输入关键词查询 Q	
yzc yzc admin sys-admin	<	Lest 测试	
	>		
共2项		共1项	
		取消 上一步 「	下—步

图 3-1- 2-1



新建访问控制策略

 \times

关联资源账户 关联账户组





图 3-1- 2-2

此时我们使用 test 帐号去登录堡垒机,可以看到,刚才我们配置的策略已 经生效,如图 3-1-3,



~											
	己匣子										🗏 🔱 lisi 🔻
-	桌面	\$ 第 / 运 纳	1 / 主机运输								
œ	运维へ	主机运	维							C	登录配置下载
		主机名称	★ ▼ 输入搜索项值词								_
	应用运输		主机名称 💠	主机地址 💠	协议 💌	标签 🔻			资源账户 👻		操作
в	Im ~		RelHat-38	192.168.13.138.22	SSH			2	[Empty]		20-20-
			CentOS-6.5	192.168.13.123:22	SSH			2	[Empty]		整荣
			CentOS-13.123	192.168.13.123.22	SFTP			2	root		20录
			11.112.12 X101-755 #1005	785					20 %/	য় 👻 < 🖬	→ 前往 1 页

图 3-1- 3

登录效果,如图 3-1-4



图 3-1-4

以上为堡垒机基础使用所需要满足的条件,简单来说分为4点:

1.堡垒机用户

2.资源主机

- 3.资源主机的系统帐号
- 4.访问策略



核心思路:通过访问策略控制指定的堡垒机用户能够在什么时候使用指定的系 统帐号访问指定的资源主机。

更多配置相关,请参考《用户手册》。