阿里云 专有云企业版

安全管理员指南

产品版本:V3.6.0

文档版本:20180824

为了无法计算的价值 | 【-】阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读 或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用于自身的合法 合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格遵守保密义务;未经阿里云 事先书面同意,您不得向任何第三方披露本手册内容或提供给任何第三方使用。
- 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分 或全部,不得以任何方式或途径进行传播和宣传。
- 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有任何通知或者 提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时发布更新后的用户文档。您 应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云文档中所有内容,包括但不限于图片、架构设计、页面布局、文字描述,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表本文档中的内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 阿里云文档中所有内容,包括但不限于图片、页面设计、文字描述,均由阿里云和/或其关联 公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云 和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发 行或公开发表本文档中的内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、 广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包

含"阿里云"、Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案 或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定 描述使第三方能够识别阿里云和/或其关联公司)。

7. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

通用约定

格式	说明	样例
•	该类警示信息将导致系统重大变更甚至 故障,或者导致人身伤害等结果。	会 禁止 : 重置操作将丢失用户配置数据。
A	该类警示信息可能导致系统重大变更甚 至故障,或者导致人身伤害等结果。	▲ 警告: 重启操作将导致业务中断,恢复业务所需 时间约10分钟。
()	用于警示信息、补充说明等,是用户必须了解的内容。	() 注意: 导出的数据中包含敏感信息,请妥善保 存。
	用于补充说明、最佳实践、窍门等,不是用户必须了解的内容。	道 说明 : 您也可以通过按 Ctrl + A 选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定 。
courier 字体	命令。	执行 cd /d C:/windows 命令,进 入Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid Instance_ID
[]或者[a b]	表示可选项,至多选择一个。	ipconfig[-all/-t]
{}或者{a b}	表示必选项,至多选择一个。	<pre>swich {stand slave}</pre>

目录

法律声明	I
通用约定	
1 4/2 早二氏	1
2 使用须知	2
3 快速入门	3
3.1 用户权限说明	3
3.2 登录云盾安全中心	3
3.3 退出云盾安全中心	4
3.4 云盾安全中心界面	5
4 态势感知	7
4.1 总览	7
4.1.1 查看安全总览信息	7
4.1.2 查看网络流量信息	9
4.1.3 查看访问分析结果	10
4.1.4 查看可视化大屏	
4.2 事件分析	
4.2.1 查看紧急事件	14
4.3 威胁分析	15
4.3.1 查看威胁分析结果	16
4.3.2 查看威胁攻击信息	17
4.4 安全报表	
4.4.1 添加报表任务	19
4.4.2 管理报表任务	21
4.5 漏洞扫描	
4.5.1 查看漏洞信息	22
4.5.2 查看弱口令信息	
4.5.3 添加自定义弱口令	24
4.5.4 查看配置项检测结果	
5 网络安全	28
5.1 启用网络安全阻断功能	28
6 应用安全	29
6.1 Web应用防火墙	
6.1.1 限制说明	
6.1.2 配置域名接入	29
6.1.2.1 开始之前	

	6.1.2.2 添加防护域名	
	6.1.2.3 上传HTTPS证书和私钥(仅针对HTTPS站点域名)	
	6.1.2.4 放行Web应用防火墙VIP	
	6.1.2.5 本地验证域名Web应用防火墙接入配置	35
	6.1.2.6 修改DNS解析	36
	6.1.3 配置防护功能	36
	6.1.3.1 配置Web应用攻击防护	
	6.1.3.2 配置恶意IP惩罚	38
	6.1.3.3 配置CC安全防护	39
	6.1.3.4 配置精准访问控制	42
	6.1.3.5 配置封禁地区	45
	6.1.4 查看安全报表	46
	6.1.4.1 查看安全总览	46
	6.1.4.2 查看安全报表	47
	6.1.4.3 查看业务分析	49
7	云主机安全	51
	7.1 主机安全总览	51
	7.2 主机列表	53
	7.2.1 管理主机列表	53
	7.2.2 管理分组	54
	7.3 安全预防	56
	7.3.1 漏洞管理	
	7.3.1.1 管理Linux软件漏洞	56
	7.3.1.2 管理Windows系统漏洞	57
	7.3.1.3 管理Web-CMS漏洞	59
	7.3.1.4 管理其他漏洞	60
	7.3.1.5 设置漏洞管理策略	62
	7.3.2 基线检查	63
	7.3.2.1 基线检查介绍	63
	7.3.2.2 管理基线检查	64
	7.3.2.3 设置基线检查策略	65
	7.4 入侵检测	65
	7.4.1 异常登录	65
	7.4.1.1 查看异常登录	66
	7.4.1.2 设置登录安全策略	67
	7.4.2 网站后门	68
	7.4.2.1 管理网站后门	68
	7.4.3 主机异常	69
	7.4.3.1 管理主机异常	69
	7.5 主机指纹	69
	7.5.1 管理监听端口	69

	7.5.2 管理运行进程	70
	7.5.3 管理账号信息	70
	7.5.4 管理软件版本	71
	7.5.5 设置主机指纹刷新频率	71
	7.6 日志检索	
	7.6.1 日志检索介绍	72
	7.6.2 查询日志	73
	7.6.3 各日志源字段说明	73
	7.6.4 语法逻辑说明	78
	7.7 设置	79
	7.7.1 管理安全配置	79
	7.7.2 安装安骑士Agent插件	79
	7.7.3 卸载安骑士Agent插件	81
8 4	物理机防护	82
	8.1 查看并处理文件篡改事件记录	
	8.2 查看并处理异常进程记录	
	8.3 查看并处理异常网络连接记录	
	8.4 查看并处理异常端口监听记录	
9 }	资产总版	
-	91分组管理	85
	9.1.1 添加分组	86
	9.1.2 删除分组	
	9.1.3 调整分组排序	
	9.2 资产信息	
	9.2.1 管理主机资产	
	9.2.2 管理NAT资产	
	9.2.3 批量修改资产所属分组或区域	
10	安全审计	
-	→→→→→→→ 10.1 查看审计—监	94
	10.2 查询审计事件	95
	10.3 查看原始日志	
	10.4 策略设置	
	10.4.1 配置审计策略	
	10.4.1.1 新增审计策略	
	10.4.1.2 管理审计策略	
	10.4.2 管理操作类型	
	10.4.3 设置告警接收人	101
	10.4.4 管理事件日志存档	
	10.4.5 管理导出任务	
	10.4.6 修改系统配置	

□	105
11.1 管理阿里云账号	
11.2 云端同步	107
11.2.1 同步状态说明	
11.2.2 刷新云端同步列表	
11.2.3 设置更新方式	
11.2.4 手动更新规则库	109
11.2.5 回滚规则库	110
11.2.6 查看历史记录	
11.2.7 导入离线升级包	111
11.3 告警设置	112
11.3.1 设置告警联系人	112
11.3.2 设置告警信息	
11.4 全局设置	113
11.4.1 流量采集网段设置	113
11.4.1.1 添加流量采集网段	113
11.4.1.2 管理流量采集网段	114
11.4.2 区域设置	115
11.4.2.1 添加区域网段	
11.4.2.2 管理区域网段	
11.4.3 配置白名单	117
	110
12 可远女主厂吅	
12 り処女主/	
12 り処女主/	
12 リ処女主/ ロ 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略	
12 リ処女主/ 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值	
12 リルタエ/ ロ 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值	
 12 リレタエ/ ロー 12.1 DDoS防护… 12.1.1 查看DDoS事件… 12.1.2 DDoS防护策略… 12.1.2.1 设置预警阈值… 12.1.2.2 管理预警阈值… 12.2 云防火墙… 	
 12 リレタエ/ m 12.1 DDoS防护… 12.1.1 查看DDoS事件… 12.1.2 DDoS防护策略… 12.1.2.1 设置预警阈值… 12.1.2.2 管理预警阈值… 12.2.2 管理预警阈值… 12.2.1 开始之前… 	
 12 可见女主/ 而 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2 至防火墙 12.2.1 开始之前 12.2.2 拓扑图图例说明 	
 12 中边女主/ 而 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2.2 管理预警阈值 12.2.2 无防火墙 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.3 建立业务区 	119
 12 可见女主/ 而 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2.2 管理预警阈值 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.3 建立业务区 12.2.4 导入ECS云服务器 	
 12 中人之女主/ пп 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2.2 管理预警阈值 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.3 建立业务区 12.2.4 导入ECS云服务器 12.2.5 建立角色组,将已导入的ECS云服务器分组 	
 12 可见安主/ пп. 12.1 DDoS防护	119
 12 中边边女主/ 面 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2 管理预警阈值 12.2 云防火墙 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.2 拓扑图图例说明 12.2.3 建立业务区 12.2.4 导入ECS云服务器 12.2.5 建立角色组,将已导入的ECS云服务器分组 12.2.5.1 将已明确角色的ECS云服务器进行分组 12.2.5.2 将未明确角色的ECS云服务器进行分组 	119
 12 中以及安主/ пп. 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2.2 管理预警阈值 12.2.2 管理预警阈值 12.2.2 玩水墙 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.3 建立业务区	119
 12 可见又主/ 面 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.2 室球火墙 12.2 云防火墙 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.3 建立业务区 12.2.3 建立业务区 12.2.5 建立角色组,将已导入的ECS云服务器进行分组 12.2.5.1 将已明确角色的ECS云服务器进行分组 12.2.5 将未明确角色的ECS云服务器进行分组 12.2.6 审核流量(部署访问控制策略) 12.2.7 发布业务区(下发访问控制策略) 	119
 12 中见之父主/ пп 12.1 DDoS防护 12.1.1 查看DDoS事件 12.1.2 DDoS防护策略 12.1.2 DDoS防护策略 12.1.2.1 设置预警阈值 12.1.2.2 管理预警阈值 12.1.2.2 管理预警阈值 12.2 云防火墙 12.2.1 开始之前 12.2.2 拓扑图图例说明 12.2.2 拓扑图图例说明 12.2.3 建立业务区 12.2.4 导入ECS云服务器 12.2.5 建立角色组,将已导入的ECS云服务器分组 12.2.5.1 将已明确角色的ECS云服务器进行分组 12.2.5.2 将未明确角色的ECS云服务器进行分组 12.2.6 审核流量(部署访问控制策略) 12.2.7 发布业务区(下发访问控制策略) 12.2.8 临时使用一键全通功能 	119
 12 马边安主/ m 12.1 DDoS防护	119

12.3 堡垒机	141
12.3.1 堡垒机系统部署	142
12.3.2 admin管理员快速配置指南	143
12.3.2.1 登录云盾堡垒机系统	143
12.3.2.2 快速配置	144
12.3.2.2.1 新建用户	144
12.3.2.2.1.1 手工新建用户	145
12.3.2.2.1.2 批量导入用户	147
12.3.2.2.2 管理用户配置	148
12.3.2.2.3 新建用户组	149
12.3.2.2.4 对用户进行分组	150
12.3.2.2.5 新建主机	151
12.3.2.2.5.1 手工新建主机	151
12.3.2.2.5.2 批量导入主机	155
12.3.2.2.6 管理主机配置	155
12.3.2.2.7 新建主机组	158
12.3.2.2.8 对主机进行分组	158
12.3.2.2.9 运维授权	159
12.3.2.2.9.1 新建运维规则	159
12.3.2.2.9.2 管理运维规则	161
12.3.2.3 实时监控	165
12.3.3 运维人员操作指南	
12.3.3.1 登录云盾堡垒机系统	165
12.3.3.2 下载运维工具	166
12.3.3.3 Web方式运维操作指南	168
12.3.3.3.1 安装单点登录器	168
12.3.3.3.2 指定运维工具	169
12.3.3.3 主机运维	170
12.3.3.3.1 通过SSH协议登录主机进行运维	170
12.3.3.3.3.2 通过RDP协议登录主机进行运维	
12.3.3.3.3 通过SFTP协议登录主机进行运维	173
12.3.3.3.4 未授权登录主机进行运维	175
12.3.3.3.5 运维审批申请	176
12.3.3.4 CS方式运维操作指南	
12.3.3.4.1 苹果系统客户端运维操作指南	
12.3.3.4.1.1 准备工作	177
12.3.3.4.1.2 通过命令行终端app的菜单方式登录目标主机进行运维	177
12.3.3.4.1.3 通过远程桌面连接app的菜单方式登录目标主机进行运维	
12.3.3.4.2 Windows系统客户端运维操作指南	184
12.3.3.4.2.1 准备工作	184
12.3.3.4.2.2 通过SSH工具登录目标主机进行运维	

12.3.3.4.2.3 通过远程桌面连接工具的菜单方式登录目标主机进行运维	190
12.3.3.4.2.4 通过WinSCP工具登录目标主机进行运维	193
12.3.3.4.2.5 通过XFTP工具登录目标主机进行运维	195
12.3.4 审计管理员操作指南	199
12.3.4.1 登录云盾堡垒机系统	199
12.3.4.2 审计	200
12.3.4.2.1 会话审计	200
12.3.4.2.1.1 查看所有会话	200
12.3.4.2.1.2 搜索审计会话	202
12.3.4.2.1.3 查询事件	203
12.3.4.2.1.4 搜索事件	205
12.3.4.2.2 审计规则	206
12.3.4.2.2.1 添加审计规则	206
12.3.4.3 运维报表	208
12.3.4.3.1 按时间范围查看运维报表	208
12.3.4.3.2 设置报表自动发送	208
12.3.5 系统管理员操作指南	209
12.3.5.1 登录云盾堡垒机系统	209
12.3.5.2 系统管理	210
12.3.5.2.1 管理网络相关设置	210
12.3.5.2.2 管理认证相关配置	213
12.3.5.2.3 管理系统相关配置	216
12.3.5.2.4 管理系统存储	219
12.3.5.2.5 查看系统操作日志	221
12.3.5.2.6 查看系统报表	223
12.3.5.2.7 维护本机系统	223
12.4 数据库审计	233
12.4.1 快速部署指南	234
12.4.1.1 数据库审计系统部署	234
12.4.1.2 登录云盾数据库审计系统	237
12.4.1.3 数据库审计系统初始化	238
12.4.1.3.1 前提条件	238
12.4.1.3.2 导入License文件	238
12.4.1.3.3 添加被审计的数据库实例	239
12.4.1.3.4 部署Agent程序	241
12.4.1.3.4.1 Agent程序部署位置	241
12.4.1.3.4.2 自动部署Agent程序	242
12.4.1.3.4.3 手动部署Agent程序	243
12.4.1.3.4.4 部署测试	252
12.4.2 系统管理员指南	253
12.4.2.1 系统	253

12.4.2.1.1 证书管理	253
12.4.2.1.2 系统控制	254
12.4.2.1.3 时钟设置	255
12.4.2.1.4 安全管理	256
12.4.2.1.5 通知管理	257
12.4.2.2 监控	258
12.4.2.2.1 压力	258
12.4.2.2.2 资源与引擎	259
12.4.2.2.3 数据中心监控	260
12.4.2.2.4 异常日志	261
12.4.2.2.5 系统日志	261
12.4.3 安全管理员指南	262
12.4.3.1 概况	263
12.4.3.1.1 系统检测	263
12.4.3.1.2 数据库监控	265
12.4.3.1.2.1 添加数据库	265
12.4.3.1.2.2 管理已添加的数据库	266
12.4.3.2 数据库详细信息	267
12.4.3.2.1 概况(单库)	268
12.4.3.2.1.1 查看单数据库审计状态	268
12.4.3.2.1.2 查看单数据库详细信息概况	269
12.4.3.2.2 风险	270
12.4.3.2.2.1 查看风险统计结果	270
12.4.3.2.2.2 查看规则命中记录	271
12.4.3.2.2.3 风险语句检索及处理	275
12.4.3.2.3 语句	278
12.4.3.2.3.1 查看SQL统计	279
12.4.3.2.3.2 检索SQL语句	281
12.4.3.2.3.3 检索语句模板	283
12.4.3.2.3.4 查看执行失败的SQL语句	285
12.4.3.2.3.5 查看TopSQL语句	286
12.4.3.2.3.6 查看新型语句	288
12.4.3.2.3.7 分析访问源	289
12.4.3.2.4 会话	290
12.4.3.2.4.1 查看会话统计	290
12.4.3.2.4.2 检索会话信息	292
12.4.3.2.4.3 查看登录失败会话	293
12.4.3.2.4.4 查看活跃会话	294
12.4.3.2.4.5 查看应用会话	295
12.4.3.2.5 报表(单库)	296
12.4.3.2.5.1 查看报表(单库)	296

12.4.3.2.5.2 管理定时推送任务(单库)	298
12.4.3.2.6 规则	299
12.4.3.2.6.1 优先级视图下管理信任语句	300
12.4.3.2.6.2 优先级视图下管理信任规则	301
12.4.3.2.6.3 优先级视图下管理敏感语句	304
12.4.3.2.6.4 优先级视图下管理SQL注入规则	304
12.4.3.2.6.5 优先级视图下管理风险操作规则	305
12.4.3.2.6.6 分类视图下管理风险操作规则	307
12.4.3.2.6.7 分类视图下管理SQL注入规则	
12.4.3.2.6.8 分类视图下语句管理	309
12.4.3.2.7 配置(单库)	310
12.4.3.2.7.1 配置单库的规则告警通知	
12.4.3.3 报表	311
12.4.3.3.1 查看报表	
12.4.3.3.2 管理定时推送任务	312
12.4.3.4 系统告警信息	
12.4.3.4.1 查看系统告警信息	313
12.4.3.4.2 配置系统告警	
12.4.3.5 配置	315
12.4.3.5.1 授权管理	
12.4.3.5.1.1 用户管理	
12.4.3.5.1.2 功能授权	
12.4.3.5.2 IP名称管理	318
12.4.3.6 维护	319
12.4.3.6.1 数据备份恢复	
12.4.3.6.1.1 设置自动备份	
12.4.3.6.1.2 手动备份与恢复	320
12.4.3.6.1.3 查询备份清单	
12.4.3.6.2 Agent管理	
12.4.3.6.2.1 下载Agent	
12.4.3.6.2.2 Agent自动部署	322
12.4.3.6.3 恢复出厂设置	
12.4.3.6.4 引擎管理	
12.4.4 审计管理员指南	325
12.4.4.1 查看系统操作日志	325
12.5 数据发现与脱敏	
12.5.1 登录专有云数据安全控制台	326
12.5.2 专有云数据安全控制台界面	327
12.5.3 使用指南	
12.5.3.1 数据源管理	328
12.5.3.1.1 数据库	328

12.5.3.1.1.1 添加数据库	328
12.5.3.1.1.2 修改数据库	329
12.5.3.1.1.3 删除数据库	330
12.5.3.1.1.4 查询数据库	331
12.5.3.1.2 文件源	332
12.5.3.1.2.1 添加文件源	332
12.5.3.1.2.2 添加文件	
12.5.3.1.2.3 修改文件	
12.5.3.1.2.4 删除文件	
12.5.3.1.2.5 修改文件源	338
12.5.3.1.2.6 删除文件源	339
12.5.3.1.2.7 查询文件源	340
12.5.3.2 数据发现	
12.5.3.2.1 发现任务	
12.5.3.2.1.1 数据库发现任务	341
12.5.3.2.1.2 文件发现任务	351
12.5.3.2.1.3 查询发现任务	
12.5.3.2.2 敏感字段梳理	
12.5.3.2.2.1 添加敏感数据源	361
12.5.3.2.2.2 核实敏感数据	
12.5.3.2.2.3 设置为非敏感数据	363
12.5.3.2.2.4 修正敏感数据	
12.5.3.2.2.5 查询敏感数据	
12.5.3.2.3 敏感文件梳理	
12.5.3.2.3.1 核实敏感数据	
12.5.3.2.3.2 设置为非敏感数据	367
12.5.3.2.3.3 修正敏感数据	
12.5.3.2.3.4 查询敏感数据	
12.5.3.2.4 发现规则	
12.5.3.2.4.1 查看发现规则	
12.5.3.2.4.2 添加自定义发现规则	
12.5.3.3 数据脱敏	
12.5.3.3.1 数据子集	
12.5.3.3.1.1 添加数据子集	371
12.5.3.3.1.2 编辑数据子集	
12.5.3.3.1.3 删除数据子集	
12.5.3.3.2 数据关系	
12.5.3.3.2.1 查看数据关系	
12.5.3.3.3 脱敏方案	
12.5.3.3.3.1 添加数据库脱敏方案	
12.5.3.3.3.2 添加文件脱敏方案	381

12.5.3.3.3.9 修改脱敏方案	384
12.5.3.3.3.4 删除脱敏方案	385
12.5.3.3.4 脱敏任务	386
12.5.3.3.4.1 数据库脱敏任务	386
12.5.3.3.4.2 文件脱敏任务	395
12.5.3.3.4.3 查询脱敏任务	404
12.5.3.3.5 脱敏算法	404
12.5.3.3.5.1 查看脱敏算法	404
12.5.3.3.5.2 添加自定义脱敏算法	404

1 什么是云盾

云盾是从网络安全、服务器安全、应用安全、数据安全和安全管理等多维度防护云上安全的一套专 有云安全解决方案。

在云计算环境下,随着技术的发展,传统以检测技术为主的边界安全防护不能充分保障云上业务的 安全。云盾结合云计算平台强大的数据分析能力以及专业的安全运营团队,从网络层、应用层、主 机层等多个层面为用户提供一体化的安全防护服务。

云盾标准版提供以下功能:

- **态势感知**:捕获和分析网络安全态势、对安全事件进行关联回溯和大数据分析,展示已发现的安全事件威胁风险。
- 网络安全:帮助安全管理员全面管理专有云平台内部、外部的网络安全状态。
- 应用安全:通过Web应用防火墙功能,帮助安全管理员保障专有云平台应用层面安全。
- 云主机安全:通过主机安全预防、入侵检测等功能,帮助安全管理员管理云主机安全。
- 物理机安全:包含文件篡改、异常进程、异常网络连接、可以端口监听等功能。
- 资产管理:帮助安全管理员管理专有云环境中的资产,包括主机资产、NAT IP资产。
- 安全审计:对云服务操作日志展示和审计,以便安全审计员及时发现并消除安全隐患。
- 系统管理:包括阿里云账号管理、云端同步、告警设置、全局设置等功能。

2 使用须知

在登录云盾安全中心前,您需要确认本地PC符合以下配置。

本地PC需要满足如表 2-1: 配置要求表中配置要求,才可以正常登录云盾安全中心。

表 2-1: 配置要求表

内容	要求
浏览器	 Internet Explorer浏览器: 11及以上版本 Chrome浏览器(推荐): 42.0.0及以上版本 Firefox浏览器: 30及以上版本 Safari浏览器: 9.0.2版本及以上版本
操作系统	 Windows XP/7 及以上版本 Mac系统

3 快速入门

3.1 用户权限说明

该章节介绍了云盾涉及的用户角色。

所有云盾安全中心角色均为默认角色,无法自定义添加。在登录云盾安全中心前,您需要确认自己的账号已经分配云盾相关的角色,具体角色说明参见表 3-1: 云盾默认角色。

表 3-1: 云盾默认角色

角色名称	角色说明	
云安全中心系统管理 员	负责云盾安全中心系统管理设置,具备阿里云账号管理、云端同步、告警 设置、及全局设置的权限。	
云安全中心安全管理 员	负责整个专有云平台的安全状态,管理云盾各功能模块的安全策略设 置,包括态势感知、网络安全、应用安全、云主机安全、物理机安全、资 产管理各目录下的所有功能节点权限。	
	说明 : Web应用防火墙、云防火墙等功能的权限需要单独开通。	
部门安全管理员	负责某个指定部门中各云产品资源的安全状态,管理针对该部门的云盾各 功能模块的安全策略设置,包括态势感知、网络安全、应用安全、云主机 安全、物理机安全、资产管理各目录下的所有功能节点权限。同时,部门 管理员还可以设置该部门中安全事件告警的联系人及告警方式。	
	说明 : Web应用防火墙、云防火墙等功能的权限需要单独开通。	
云安全中心审计员	负责整个专有云平台安全审计工作,查看审计事件、原始日志并设置相关 审计策略,具备安全审计目录下所有功能节点权限。	

如果您没有相关账号和角色,请联系管理员创建用户及授予角色,具体步骤请参考《用户指南》中创建用户一节。

3.2 登录云盾安全中心

该章节介绍了如何登录到云盾安全中心。

前提条件

登录Apsara Stack控制台前,确认您已从部署人员处获取Apsara Stack控制台的IP地址或服务域名 地址。

Apsara Stack控制台访问地址为: http:// Apsara Stack控制台的IP地址或服务域名地址/ manage。

操作步骤

- 1. 打开浏览器。
- 2. 在地址栏中,输入Apsara Stack控制台的访问地址 http:// *Apsara Stack*控制台的*IP*地址或服 务域名地址/manage,按回车键。

密码登录	
്ര mwli	
A	
安衰	

- 3. 输入正确的用户名及密码。
 - 系统有一个缺省的超级管理员,用户名是super ,密码是super ,超级管理员可以用来创建系统管理员,由系统管理员创建其他系统用户并以短信、邮件的形式通知缺省密码。
 - 首次登录Apsara Stack控制台时,需要修改登录用户名的密码,请按照提示完成密码修改。
 为提高安全性,密码必须满足最小复杂度要求,即包含英文大/小写字母(A~Z、a~z)、数字(0~9)、特殊符号(!、@、#、\$、%等)中的两种,并且密码长度为 8~20 位。
- 4. 单击登录,进入运行大盘页面。
- 5. 在页面顶部的菜单栏中,选择云管控中心 > 云基础产品 > 云盾控制台。
- 6. 选择区域,单击云盾控制台,进入云盾安全中心。

3.3 退出云盾安全中心

该章节介绍了如何退出云盾安全中心。

• 在云盾安全中心页面,单击页面右上角的退出,即可从云盾安全中心注销。

3.4 云盾安全中心界面

该章节介绍了云盾安全中心页面信息。

云盾安全中心的界面主要可以分为三大区域,如图 3-1: 云盾安全中心页面所示。

图 3-1: 云盾安全中心页面

0	云盾安全中心	3 用户中心	退出
	Ξ	意先 2	
•	态势感知		
•	网络安全	安主志见 网络细丽莲 初方代灯 当他代入并	
•	应用安全	所履区域: 全部 v	
•	云主机安全		
•	物理机安全	文化 2010日11日 2010日111日 2010日11日 <t< th=""><th></th></t<>	
•	资产管理		
•	数据安全		
•	安全审计	° -• • • • • • • • • • • • • • • • • • •	• • •
•	数据库审计		
•	堡垒机	05/04 05/06 05/08 05/10 05/12 05/14 05/16 05/18 05/20 05/22 05/24 05/26 05/28 05/30 ● 家急事件 政士 弱点	06/01
•	系统管理 1		
		最新威胁(30天)	

表 3-2: 云盾安全中心界面区域说明

序号	区域	说明	
1	导航区	云盾安全中心高级版主要功能如下:	
		 态势感知:捕获和分析网络安全态势、对安全事件进行关联回溯和大数据分析,展示已发现的安全事件威胁风险。 网络安全:帮助安全管理员全面管理专有云平台内部、外部的网络安全状态。 	
		• 应用安全 :包括Web应用防火墙功能,帮助安全管理员保障专有 云平台应用层面安全。	
		• 云主机安全 :包括安全预防、入侵检测等功能,帮助安全管理员 管理云主机安全。	
		• 物理机安全:包括文件篡改、异常进程、异常网络连接、可以端 口监听等功能。	

序号	区域	说明	
		 资产管理:帮助安全管理员管理专有云环境中的资产,包括主机资产、NAT IP资产。 安全审计:对云服务操作日志展示和审计,以便安全审计员及时发现并消除安全隐患。 系统管理:包括阿里云账号管理、云端同步、告警设置、全局设置等功能。 	
2	操作视图区	选择某功能菜单项后,该菜单项的功能配置界面将显示在右侧的操作视图区中。	
3	操作按钮区	 用户中心:单击此按钮进入个人信息页面,可查看当前登录用户的基本资料,或修改登录密码。 退出:单击此按钮退出当前登录。 	

4 态势感知

该章节介绍了态势感知概念。

态势感知全面集成了企业漏洞监控、黑客入侵监控、Web攻击监控、DDoS攻击监控、威胁情报监 控、企业安全舆情监控等安全态势监控手段,通过建模分析方法,从流量特征、主机行为、主机操 作日志等获取关键信息,识别无法单纯通过流量检测或文件查杀发现的入侵行为,借助云端分析模 型输入并结合情报数据,发现攻击威胁来源和行为,并评估威胁程度。

态势感知主要包含:

- 总览:展现安全的整体态势、网络流量情况和安全大屏相关信息。
- 事件分析:展现业务系统中已经发生的安全事件和发展趋势。
- 威胁分析:展现当前系统面临的安全风险。
- 安全报表:配置专有云平台安全报表任务。
- 漏洞扫描:展现系统中存在的漏洞和缺陷。

4.1 总览

该章节介绍了当前专有云环境的安全态势总览。

总览页面对整体安全态势进行概要性展示,以便安全管理员快速了解和掌握当前安全态势。

总览主要包括以下方面:

- **安全总览**:对系统已经发生的安全事件、目前面临的安全威胁、系统自身存在的弱点缺陷进行概要性展示。
- 网络流量:对网络的出口、入口、QPS 流量信息的分析,展示流量的高峰、低谷、速率和地域 来源的分布规律。
- 访问分析:分析前一天的访问情况,识别访问者身份,并向安全管理员展示访问者信息及访问页面信息。
- 可视化大屏:为安全管理员提供最直观的安全形势和面临威胁的展示,作为安全决策的重要参考 指标。

4.1.1 查看安全总览信息

该章节介绍了如何查看专有云平台的安全趋势、最新威胁和资产概览信息。

背景信息

安全管理员通过安全总览中的信息,全方位、整体性地把握自身系统的安全态势。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 总览,单击安全总览页签。

查看目前专有云平台安全的总览情况,如图 4-1:安全总览页面所示。

图 4-1: 安全总览页面



表 4-1: 安全总览页面区域说明表

页面区域	说明
安全趋势	安全趋势展示了当前系统已经发生的安全事件和攻击、系统发现的弱点缺陷,并从时间维度展示了系统安全态势的变化。
最新威胁	最新威胁展示了当前系统存在的安全威胁,急需安全管理员积极关注。
	说明 : 这些安全威胁事件都是由云盾的核心扫描器扫描,并通过针对专有云平台的 大数据分析模型分析所得。
资产概览	选取用户最关心的资产情况进行展示,使用户实时掌握资产状态。

3. 单击**今日紧急事件、今日攻击、今日弱点**,或查看最新威胁,可直接跳转至相应的页面查看详细 信息。

例如,单击今日紧急事件,即跳转至事件分析页面。

4.1.2 查看网络流量信息

该章节介绍了如何查看网络流量信息。

背景信息

网络流量通过折线图的形式,展示了过去一段时间的流量信息。安全管理员通过查看不同时期、区域或单个IP的流量情况,可以定位流量的高峰和低谷时间、速率和地域等流量分布规律;同时通过 查看TOP5流量的IP,甄别恶意的IP访问。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 总览,单击网络流量页签。
- 3. (可选)选择**所属区域**,输入ECS实例IP,单击**搜索**。 此步骤用于分区域、分IP查询流量信息。
- 4. (可选)单击**今天、最近30天、最近90天**。

此步骤用于切换查看不同时间段的流量信息。

- 5. 查看某时间节点具体流量信息。
 - 在网络出/入口流量图中,将鼠标停留在流量折线上,可查看该时间点出口或入口流量的详细 信息及流量TOP5的IP,如图 4-2: 查看流量 TOP5的 IP所示。



图 4-2: 查看流量 TOP5 的 IP

• 在QPS(平均)图中,将鼠标停留在流量折线上,可查看该时间点的具体QPS信息,如图 4-3: 查看QPS详细信息所示。

图 4-3: 查看QPS详细信息



4.1.3 查看访问分析结果

该章节介绍了如何查看访问分析结果。

背景信息

访问分析:对不同来源的访问,通过大数据分析,甄别出正常访问、恶意访问和爬虫访问三种类型。安全管理员可以根据恶意访问和爬虫访问的行为,了解自身系统可能面临的安全问题来源。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 总览,单击访问分析页签。

查看访问分析页面。

表 4-2: 访问分析页面

区域	说明
昨日全局访问	展示昨日访问最多的Top10域名和访问IP数。
昨日访问者识别	展示昨日正常访问、恶意访问和爬虫访问数量的统计信息。
历史明细列表	展示恶意访问和爬虫访问的历史信息。

3. 在历史明细列表中,单击全部、恶意访问、爬虫访问。

查看详细访问信息。

表 4-3: 详细访问信息

参数	说明
来访者IP	来访的IP信息。
识别类型	来访类型:恶意访问、爬虫访问。
发生时间	来访发生时间。
UserAgent	来访HTTP报文中的User-Agent信息。
目标应用	访问目标URL信息。
访问页面个数	统计访问的页面数量。
最高每秒访问次数	最高每秒访问次数。
本次访问是否有Web攻击	检查访问是否存在Web攻击。

4.1.4 查看可视化大屏

该章节介绍了如何查看可视化大屏。

背景信息

可视化大屏通过形象生动的动画效果,展示关键性的安全事件指标。安全管理员能够一目了然地掌握当前的整体安全态势,为安全决策提供有效支持。

可视化大屏包括:互联网边界流量安全监控大屏、业务安全态势和评分大屏。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 总览,单击可视化大屏页签。

图 4-4: 可视化大屏页面



单击**修改**,修改**互联网边界流量安全监控**的标题。

3. 单击**互联网边界流量安全监控**屏幕。

查看互联网边界流量安全监控大屏信息。



互联网边界流量安全监控大屏对目前的请求和攻击的来源地域、数量进行统计;同时也展示系统 目前流量的整体情况。通过列出的TOP5的请求和攻击地域,安全管理员能够对请求的压力来源 和攻击的地域分布有准确的了解,及时掌握攻击分布的地域规律。

表 4-4: 访问流量数据来源表

类型	实现的机制
请求分析	将用户关注的资产推送给流量安全监控模块,流量安全监控模块根据需要关注的资产上报这些资产被访问的情况。
攻击分析	由云盾流量安全监控模块检测,针对于类似Web攻击的事件进行上报和展示。
流量展示	由流量安全监控模块收集流量信息并上报给控制台记录。

4. 单击业务安全态势和评分屏幕。

查看业务安全态势和评分大屏信息。



业务安全态势和评分大屏是对当前系统面临的安全事件的详细呈现。通过对系统弱点缺陷、遭受 攻击和黑客重点关注资产的分析,为系统的安全状况进行打分评价,提示目前系统的安全等级。 此大屏的数据主要是云盾流量安全监控、安骑士和弱点分析等模块进行扫描并上报。TOP5黑客 最感兴趣资产由大数据引擎通过模型分析获得。

4.2 事件分析

该章节介绍了当前专有云环境的紧急事件分析。

紧急事件是系统中已经或正在发生的安全事件。紧急事件被云盾的流量安全监控、安骑士、弱点分 析等功能模块扫描发现并上报,安全管理员需要关注并采取安全措施。

紧急事件中包括的事件类型和含义请参见表 4-5: 紧急事件类型。

紧急事件类型	说明	
肉鸡行为	用户的主机被黑客控制沦为肉鸡,并对外进行攻击。	
暴力破解成功	当发现暴力破解行为和暴力破解成功时,安骑士客户端都会上报信息。其中暴 力破解成功的事件会显示在紧急事件中,安全管理员需要紧急处理。	
后门	安骑士客户端检测出系统中的Webshell后门;大数据分析模块通过对流量安全 监控模块导入的流量进行分析,检测出一句话木马和多功能木马。	
DDoS	流量安全监控模块检测出DDoS攻击。	
异常网络连接	基于各安全功能模块上报的信息,通过大数据分析模型,发现异常的向外连 接、执行恶意程序下载、恶意文件下载等行为。	
未授权下载	从流量安全监控模块输出的流量中,选择出较为特别的、数量在特定范围 内(大于1小于20)的response进行筛选,通过大数据分析模型分析出未授权 下载的情况。	
黑客工具	基于安骑士模块上报的信息,发现主机上残留的黑客工具及黑客攻击行为。	
网络流量异常	基于流量安全监控模块及安骑士模块上报的信息,发现挖矿程序等。	

表 4-5: 紧急事件类型

4.2.1 查看紧急事件

该章节介绍了如何查看紧急事件。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**态势感知 > 事件分析**。

图 4-5: 事件分析页面

事件分析				
所屬区域: 全部 🔻				
最近30日紧急事件趋势		今日事件	最近30日紧急事件分布	
600		16		
200			∰ば30天 3704 案急事件)
00 03/12 03/14 03/16 03/18 03/20 03/	• • • • • • • • • • • • • • • • • • •	01 04/03 04/05 04/07 04/09	📕 后门 🛑 DDoS 📕 异常网络连接	- 黑客工具 - 网络流星异常
黄型: 全部(3738) 肉鸡行为(1) 最力破解成功(0) 后门(3048) DDoS(636	异常网络连接(2) 未授权下载(0) 黑霄王昌(2) 网络流量	异常 (49)		
请输入要搜索的关键字				
事件关型 受影响资产	事件描述		发生时间	高级分析
DDoS NA	遭受峰值流量为193M的DDoS攻击		2018-04-10 15:35:55	
被攻击资产: (NAT)		修值流量:	193Mbps	
所匯用户:		开始时间:	2018-04-10 15:35:55	
所赋业务:默认分组		结束时间:	-	
所運区域: ci		报文峰值:	185899个/s	
该资产历史最高攻击量: 0Mbps		攻击响应状态:	-	

3. 在类型中,单击具体紧急事件类型。

列表展示该指定类型的紧急事件。各紧急事件类型说明参见表 4-5: 紧急事件类型。

4. 在列表中,查看事件具体信息。

4.3 威胁分析

该章节介绍了当前专有云环境的威胁分析,包括威胁分析和攻击两类。

威胁分析

通过对流量信息进行大数据模型分析,发现攻击特征,并按攻击行为进行整合,展示当前系统面临的安全风险。

威胁分析主要包括以下几个方面:

- 展示普通攻击和针对性攻击的最近7日攻击趋势和最近30天攻击分析。
- TOP5黑客最感兴趣的资产:通过大数据模型分析处理,按照各个资产受到的威胁的得分大小,选择威胁得分最高的五个资产进行展示,以便安全管理员对这些资产进行重点关注和保护。
- 针对性攻击分析:通过大数据模型对流量安全监控模块提供的流量信息进行分析,分析和甄别出 针对性攻击。

攻击

攻击主要包括应用攻击和暴力破解两类:

- **应用攻击**:访问Web服务器的流量都会经过云盾的流量安全监控模块,该模块将对流量进行监测,提取流量中的攻击信息。
- **暴力破解**:当黑客针对某个资产进行暴力破解的时候,安骑士客户端能够及时监测到暴力破解行为的发生并上报给控制台。

4.3.1 查看威胁分析结果

该章节介绍了如何查看威胁分析结果。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 威胁分析,选择威胁分析页签。

查看威胁分析情况。

表 4-6: 威胁分析情况

项目	说明
最近7日攻击趋势	了解专有云平台上的主机、应用近期遭受的攻击。
最近30日攻击分析	了解专有云平台上的主机、应用近期遭受的攻击。
TOP5黑客最感兴趣资产IP	资产IP是由云盾安全中心基于检测到的攻击、威胁信息通过大数据计算模型分析得出,建议安全管理员着重加固这些资产的安全防护。
针对性攻击分析	查看云盾安全中心检测到的指定类型的针对性攻击。

3. 在类型中,选择指定的针对性攻击类型。

列表展示该指定类型的针对性攻击事件。各针对性攻击类型说明参见表 4-7:针对性攻击类型。

表 4-7: 针对性攻击类型

针对性攻击类型	说明
定点Web攻击	定点Web攻击是有明显针对性的Web攻击,这意味着相对于其 他用户,黑客更关心特定的Web站点,对该Web站点进行SQL 注入、命令执行、目录扫描等恶意操作。
针对性主机密码爆破	针对性主机密码爆破是明显针对用户的登录密码的暴力破解。 通常黑客会无目标的破解主机密码,这种针对性的攻击往往暗 示黑客想攻陷特定用户的资产。

针对性攻击类型	说明
撞库攻击	通过对异常登录分析,检测出类似撞库攻击的登录行为。黑客 可能正在使用互联网上泄露的用户名密码组合尝试暴力登录用 户的网站,一旦成功将会导致用户利益遭受损失。
CMS异常登录	检测到应用的管理后台存在的异地登录事件。如果本次登录不 是用户本人操作,那么黑客可能已经窃取到后台密码,建议用 户检查密码是否存在弱口令,并尽快修改现有密码。
扫描器攻击	检测黑客使用漏洞扫描工具扫描专有云平台中主机的行为,黑 客发现漏洞后很可能对存在漏洞的主机发起针对性攻击。
pingback被恶意利用	检测攻击者利用pingback存在的漏洞发起的针对性攻击。
批量账号登录	检测攻击者使用大量的低质量账号登录的行为,而这批账号很可能是僵尸账号。

4. 在针对性攻击分析列表中,单击**查看**。

可查看本次针对性攻击的详细信息及解决方案。

4.3.2 查看威胁攻击信息

该章节介绍了如何查看威胁攻击信息。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 威胁分析页面,选择攻击页签。
- 3. 选择所属区域,单击应用攻击。

查看应用攻击情况。

表 4-8: 应用攻击情况

项目	说明		
最近7日攻击趋势	了解专有云平台上的应用近期遭受的攻击。		
最近7日攻击类型	了解专有云平台上的应用近期遭受的攻击。		
应用攻击列表	查看应用攻击事件。		

在类型中,单击应用攻击类型。

列表展示对应应用攻击类型的攻击事件。各攻击类型说明参见表 4-9: 应用攻击类型。

表 4-9: 应用攻击类型

应用攻击类型	说明	
SQL注入	Web应用程序没有对用户输入数据的合法性进行判断,攻击者通Web页面的输入区域(如URL、表单等) ,用精心构造的SQL语 句插入特殊字符和指令,通过和数据库交互获得私密信息或者篡数据库信息。	
XSS攻击	Web应用程序时没有对用户提交的语句和变量进行过滤或限制,攻 击者通过Web页面的输入区域向数据库或HTML页面中提交恶意代 码,当用户打开有恶意代码的链接或页面时,恶意代码通过浏览器 自动执行,从而达到攻击的目的。	
代码/命令执行	攻击者通过URL发起请求,在Web服务器端执行未授权的代码或命 令,从而达到攻击的目的。	
本地/远程文件包含	攻击者向Web服务器发送请求时,在URL添加非法参数,Web服务 器端程序变量过滤不严,把非法的文件名作为参数处理。这些非法 的文件名可以是服务器本地的某个文件,也可以是远端的某个恶意 文件。由于这种漏洞是由PHP变量过滤不严导致的,所以只有基于 PHP开发的Web应用程序才有可能存在文件包含漏洞。	
脚本木马	webshell,以ASP、PHP、JSP等网页文件形式存在的一种命令执 行环境,也可以将其称做为一种网页后门。攻击者在入侵了一个 网站后,通常会将ASP或PHP后门文件与网站服务器WEB目录下 正常的网页文件混在一起,然后就可以使用浏览器来访问ASP或者 PHP后门,得到一个命令执行环境,以达到控制网站服务器的目 的。	
上传漏洞	Web应用程序在处理用户上传的文件时,没有判断文件的扩展名是 否在允许的范围内,或者没检测文件内容的合法性,就把文件保存 在服务器上,甚至上传脚本木马到Web服务器上,直接控制Web服 务器。	
路径遍历	攻击者向Web服务器发送请求,通过在URL中或在有特殊意义的目 录中附加../及其变形,导致攻击者能够访问未授权的目录,或者 在Web服务器的根目录以外执行命令。	
拒绝服务	其目的在于使目标主机的网络或系统资源耗尽,使服务暂时中断或 停止,导致其正常用户无法访问。	
越权访问	应用在检查授权时存在纰漏,使得攻击者可以利用一些方式绕过权限检查,访问或者操作到原本无权访问的代码。	
其他	其他一些应用攻击类型。	

4. 选择所属区域,单击暴力破解。

查看暴力破解事件。

图 4-6: 暴力破解

所属区域: 全部	 攻击分类: 应用攻击 暴力改禁 			
和地人民民和日本地子				
英型	威胁来源/受害资产	前次发现时间	最后发现时间	损作
暴力破解	(HOST)192.168.76.118	2018-01-08 17:24:05	2018-01-08 17:24:05	<u>收起 *</u>
	被攻击资产: (HOST)192.168.76.118		攻击者印: 10	
	所题用户: yundun_test02		攻击使用协议:	
	所履业务:默认分组		发起爆破穴数:1	
	所属区域: cn-hangzhou-env6-d01			
暴力破解	(HOST)192.168.76.118	2017-12-27 12:54:14	2018-01-08 14:40:35	展开▼
暴力破解	(HOST)192.168.2.156	2018-01-07 17:08:20	2018-01-07 17:22:01	展开▼
暴力破解	(HOST)10.	2018-01-07 16:10:11	2018-01-07 16:10:11	展开▼

选择暴力破解事件事件,单击展开,可查看该暴力破解事件的详细信息。

4.4 安全报表

态势感知提供安全报表功能,支持定期将专有云平台的安全状况发送至指定邮箱,帮助安全管理员 了解当前安全态势。

安全报表可选择发送以下内容:

- 态势感知
 - 安全统计:包括态势感知总览页面展示的安全总览信息,参见查看安全总览信息。
 - 重点关注:包括态势感知事件分析页面展示的需要重点关注的紧急事件信息,参见事件分析。
 - 威胁趋势:包括网络安全威胁感知页面展示的攻击趋势、攻击分析等信息,参见威胁分析。
- 安全防护
 - DDoS:云盾安全中心发现的DDoS攻击事件信息,参见DDoS事件。
 - 主机安全:云盾安全中心发现的主机安全漏洞、异常登录、暴力破解攻击、配置风险项等信息,参见主机安全。
 - 防护资产:云盾安全中心已防护的资产信息,包括主机资产和NAT资产,参见资产总览。

4.4.1 添加报表任务

操作步骤

1. 登录云盾安全中心。

2. 定位到态势感知 > 安全报表,进入报表任务页面,如图 4-7:报表任务页面所示。

图 4-7: 报表任务页面

报表任务							
请输入报表名称 造词					đi	增任	务
报表名称	报表描述	报表类型	报告格式	发送状态			操作
00000000000000000000000000000000000000	10103	日报表	html	开启	编辑 景	1100日	详情
86	38.	日报表	html	开启	编辑 册	BRA	详情
servedal		周报表	html	开启	编辑丨册	除	详情
				Total: 3 item(s), Per Page: 20 item(s) «	1	>	30

- 3. 单击新增任务,添加报表任务。
- 4. 在添加报表任务对话框中,填写报表各项信息,如图 4-8: 添加报表任务所示。

图 4-8: 添加报表任务

添加报表任务			×
报表名称	请输入报表名称,不	超过64字符	
循环周期	日报表	Ŧ]
发送状态	□ 开启	输出格式 🔲 HTML	
报表内容	态勢感知 □ 安全统计 □ 重点关注 □ 威胁趋势	安全防护 DDoS 主机安全 防护资产	
接收邮箱	輸入邮箱		添加
报表描述	输入内容不超过10	24位	
			确定 取消


说明:

单击接收邮箱右侧的添加可添加更多邮箱地址,最多支持输入10个邮箱地址。

5. 单击**确定**。

报表任务添加成功后,指定的邮箱地址将根据设定的周期收到安全报表,如图 4-9:安全报表所 示。

图 4-9: 安全报表

态势感知							
安全统计							
				今日安全得	紛	31 /	}
今日安全统计							
异常网络连接	0 次	DDoS攻击	1 次	未授权下载	0 次	非法登录	0 次
页面被篡改	0 次	web应用攻击	395次	发现后门	4 个	暴力破解成功	3次
肉鸡行为	1 次	发现漏洞	0 个	发现弱口令	0 个	新发现资产	81 个
重点关注							
TOP10 今日緊急事件							
事件类型:肉鸡行为		受影响	资产:(HOST)10	20.216.016			
事件描述 : 暂时无法 多数据	达确定入侵原	因 , 需更 类型 :	对外DDoS				
原因:		肉鸡攻	击目标: 10.				

4.4.2 管理报表任务

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 安全报表,进入报表任务页面。
- 3. 管理已添加的报表任务。

- 选择报表任务,单击详情,查看该任务详情。
- 选择报表任务,单击编辑,可修改该报表任务。
- 选择报表任务,单击删除,可删除该报表任务。

4.5 漏洞扫描

漏洞扫描页面主要展示系统中存在的漏洞和缺陷。这些弱点有可能被黑客利用,进行非法的操 作,需要安全管理员及时消除弱点,提升系统的安全性。

漏洞扫描页面主要包括以下三类弱点:

漏洞

- 应用漏洞:弱点分析模块依赖扫描引擎具备的规则对云服务器上安装的应用程序进行扫描,并上报发现的缺陷信息。
- 主机漏洞:扫描主机系统中自身存在的漏洞,由安骑士模块检测到并上报。
- **弱口令**:检测用户资产中简单的、容易被人猜测到或破解的口令,以便提醒安全管理员及时修改 用户名和密码,提升用户密码的复杂度。

弱口令对于用户系统来说是巨大的安全隐患,建议在对系统和应用设置账户的时候,尽可能的增加密码的复杂度(例如,密码中必须包含数字、字符、特殊字符,增加密码的长度等等),同时 对密码进行分级管理;针对重要密码(例如SSH登录的用户名和密码),必须增加复杂度,同时 定期进行更换。

自定义弱口令:对于不同的用户,除了通用用户名和密码,还可能由于用户特点采用特定的用户 名和密码,云盾支持用户自定义弱口令规则,可以将用户经常使用的用户名和密码添加到弱点分 析模块的扫描规则中,实现对用户系统个性化的弱口令扫描。

配置项检测:如果用户的系统配置文件或者敏感文件存放位置不当,攻击者可能在未授权的情况下获得这些文件,导致用户关键信息的泄露。弱点分析模块对用户系统中的配置文件进行扫描,并提示可能被未授权访问的配置项文件。

4.5.1 查看漏洞信息

背景信息

漏洞分为应用漏洞和主机漏洞:

- 应用漏洞是指安装的应用程序存在的漏洞,由漏扫模块扫描并上报。
- 主机漏洞是主机本身存在的漏洞信息,由安骑士模块扫描并上报。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 漏洞扫描。
- 3. 选择所属区域,查看该区域的漏洞信息。
- 4. 选择应用漏洞分类,查看并修复应用漏洞。

应用漏洞页面显示最近七天的应用漏洞分析和具体的应用漏洞信息,如图 4-10: 应用漏洞页面所示。

图 4-10: 应用漏洞页面



- a) 在应用漏洞记录区域,选择云盾检测到的应用漏洞记录,单击相应的修复方案按钮,可查看 针对该漏洞的推荐修复方案。
- b)漏洞修复完成后,单击**马上验证**,可以向弱点分析模块发出验证信息,立即校验当前漏洞的修复状态。
- 5. 选择主机漏洞分类,查看主机漏洞信息,如图 4-11: 主机漏洞页面所示。

图 4-11: 主机漏洞页面

RR ROO NEEDER							
10421 188 - 188 - 1981 10421							98
0801	69	NIELR	//2214	展月三句	ARTICL.	87944	#JR14.0
 2016-04-15 14:37:50 	10.0000.00	用式展览器	大利用	代7集局月末2	共產文件部項	8.8	#R9
 2016-04-16 12:37:50 	10.0000.00	REAR	2,415,8	代了整用月末2	死皇文中部设	8.8	620
 2016-04-15 16:37:50 	10.0000	形式展示器	大州市府	代丁集用月末2	代集文中部设	8.8	620
 2016-08-15 16:37:20 	10.00000	Rickow	大州市港	代丁集用月22	死魔文州御道	8.0	CR+
 2017-01-25 14:37:50 	the short of	形式展現器	大利的建	代7集用月22	代集文中部设	8.0	620
 2017-01-15 13:37:50 	10.0000.00	READ	2,468	代了集局月末2	死星文件描述	8.0	220
 2016-04-15 14:37:50 	10.0000.00	形式展示器	天河北南	死了集團月4日	网络北州部设	88	630 C

在主机漏洞页面,单击右上方的导出,可将云盾检测到的主机漏洞记录导出到本地。

送明:

此页面的主机漏洞信息由安骑士模块上报,对主机漏洞的具体操作请参见漏洞管理。

4.5.2 查看弱口令信息

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 漏洞扫描。
- 3. 选择弱口令, 查看已检测到的弱口令信息, 如。图 4-12: 弱口令页面所示。

图 4-12: 弱口令页面

展示 目中 配面や加速 WESSAL ・ 協介: (2007) E888(0) RAL ・ (2007) E888(0) RAL · (2007) E888(0)

4. 选择发现的弱口令记录,单击展开,查看详细信息,如图 4-13: 弱口令详细信息所示。

图 4-13: 弱口令详细信息

	MONLOCADA JIAJ
韓口令 (NAT)10. 2017-12-27 21:30:26	2018-01-09 13:04:49
※型: 登录波/#第日令	用户槛: anonymous
密词: ******	使用协议: FTP
后台地址: 10	所腿用户:
所屋业等: 默认分娩	所履区域: cn-hangzhou-env6-d01

5. 单击忽略,可忽略该弱口令提示,且针对该弱口令将不再检测上报。

选择查看已忽略的弱口令记录,单击恢复,即可恢复对该弱口令的检测。

4.5.3 添加自定义弱口令

云盾支持自定义弱口令规则,可以将用户经常使用的用户名和密码添加到弱点分析模块的扫描规则

中,发现特定的弱口令。

操作步骤

1. 登录云盾安全中心。

- 2. 定位到态势感知 > 漏洞扫描,选择弱口令页签。
- 3. 单击自定义弱口令,可自定义针对性的弱口令规则,如图 4-14: 自定义弱口令页面所示。

图 4-14: 自定义弱口令页面

● 自定文弱口令 t 送回上吸列目	8			
请输入要查询的协议。英型或者内容	B B			湖加 导出
协议	共型	内容	活动时间	操作
fp	password	1234	2016-08-03 14:15:17	伊政 創除
fp	password	12345678	2016-08-03 14:15:17	律政 對除
fo	password	root	2016-08-03 14:15:17	律政 動除
fp	username	anonymous	2016-08-03 14:15:17	律政 劇除
fp	username	fo	2016-08-03 14:15:17	律政 動除
fp	username	test	2016-08-03 14:15:17	律政 對除
fp	username	user	2016-08-03 14:15:17	律政 對除

自定义弱口令页面显示目前弱点分析模块已经配置生效的弱用户名和弱密码。

4. 单击添加,在添加弱口令对话框中设置弱口令规则,如图 4-15: 添加弱口令对话框所示。

添加弱口令		\times
协议	ftp •	
类型	密码 *	
内容	admin;12345;88888	
说明	1、您可以按照 口令A;口令B;模式进行添加,以; 作为口令之间的隔位符 2、一次最多添加30个口令	
	确定	取消

图 4-15: 添加弱口令对话框

5. 单击确定,并再次在提示弹窗中单击确定。

- 6. 检查已添加的弱口令规则。
 - 单击修改,修改弱口令或弱用户名内容。

- 单击删除,删除不需要的弱口令规则。
- 7. 单击导出,生成并下载新的弱口令配置文件。

一般情况下,文件保存路径为C:\Users\用户名\Downloads,下载的文件为zip格式的压缩包,无需进行解压。

8. 压缩包上传至弱点分析Cactus-keeper模块的master工程所在的系统,例如上传到/root/war//目录下,执行脚本cactusConfig.sh,如图 4-16: 执行脚本界面所示。

图 4-16: 执行脚本界面

```
[root@spark2 cactusConfig]# ./cactusConfig.sh
975550d3af6d
/root/war
Archive: cactus_config_2016-10-28.zip
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ftp_user.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus config/dic ftp psw.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus config/dic mysgl user.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mysql_psw.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ssh_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ssh_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus config/dic mssgl user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus config/dic mssql psw.txt
65c5671c8259
cactus config 2016-10-28.zip
Archive: /home/datal/yundun/cactus-keeper/cactus config.zip
  inflating: /home/datal/yundun/cactus-keeper/cactus config/dic ftp user.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ftp_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mysql_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus config/dic mysql psw.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus config/dic ssh user.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus config/dic ssh psw.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus config/dic mssql user.txt
 inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mssql_psw.txt
commad.sh
done!
[root@spark2 cactusConfig]#
```

脚本执行完成后,新添加的弱口令规则即生效。

4.5.4 查看配置项检测结果

配置项检测页面显示弱点分析模块扫描到的配置项泄露的地址。

背景信息

黑客在未授权的情形下访问该地址,可能获取用户的敏感信息,造成信息泄露。安全管理员需要根据扫描检测结果,及时对存放有配置文件的目录添加权限或者将敏感文件转移至安全目录。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到态势感知 > 漏洞扫描。
- 3. 选择配置项检测页签,查看已检测到的配置项弱点,如图 4-17: 配置项检测页面所示。

图 4-17: 配置项检测页面

第月 第日中 配置符8	2NI			
所屬区域: 全部	▼ 資作: 全部(1) 已加坡(0)			
请输入要搜索的关键字				
英型	威胁来源/受害资产	前次发现时间	量后发现时间	操作
信息泄露	10	2017-12-27 21:30:26	2018-01-02 20:35:09	忽略 扁开-

4. 选择发现的配置项弱点记录,单击展开,查看详细信息,如图 4-18: 配置项弱点详细信息所示。

图 4-18: 配置项弱点详细信息

與型	威胁朱璟/反害资产	爾次說現时间	最后发现时间		操作
信息过露	10	2017-12-27 21:30:26	2018-01-02 20:35:09	9	SH 02*
	治靈河型: 备份文件泄露		波羅地	102: http://10. 8060//www.zip	
	所羅用^:		所屬並	明:默认分组	
	所服区域: cn-hangzhou-env6-d01				

5. 单击忽略,可忽略该配置项弱点提示,且针对该配置项将不再检测上报。

选择查看已忽略的配置项记录,单击恢复,即可恢复对该配置项的检测。

5 网络安全

5.1 启用网络安全阻断功能

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 安全功能设置。
- 3. 单击web攻击阻断、暴力破解阻断开关,开启或关闭相关功能,如图 5-1: 阻断开关设置所示。



关闭阻断开关后,相应的拦截功能将被禁用,仅提供预警功能。

图 5-1: 阻断开关设置

阻断开关			
类别	状态	描述	擬作
web攻击阻断	已开启	WEB攻击拦截功能已开启!	
暴力破解阻断	已开启	暴力破解攻击拦截功能已开启!	
			Total: 2 item(s) , Per Page: 20 item(s)

6 应用安全

6.1 Web应用防火墙

Web应用防火墙 (简称WAF),是阿里云自主研发的一款网站安全防护产品,它能够保护网站的应用 程序避免遭受常见Web漏洞的攻击。这类攻击既有诸如SQL注入、XSS跨站脚本等常见 Web应用攻 击,也有CC这种影响网站可用性的资源消耗型攻击。同时,它也允许根据网站实际业务制定精准的 防护策略,用于过滤对您网站有恶意的Web请求。

专有云云盾WAF防护的流量定位在HTTP/HTTPS的网站业务上。支持用户在WAF的管理界面中自 主导入证书与私钥,从而实现业务的全链路加密,避免数据在链路中被监听的可能。同时,也满足 了对HTTPS业务的安全防护需求。

6.1.1 限制说明

Web应用防火墙存在以下使用限制:

- 支持最多100个域名的接入防护,支持泛域名,不限一二级域名。
- 仅支持HTTP 80端口、 HTTPS 443端口的域名防护。

6.1.2 配置域名接入

参考以下流程将需要防护的域名配置接入Web应用防火墙。



6.1.2.1 开始之前

在使用Web应用防火墙前,请准备以下信息:

- 需要防护的域名信息,不能直接使用IP。
- 源站IP,一般为真实服务器IP。

∐ 说明 :

Web应用防火墙支持为同一域名配置多个源站IP,最多支持20个源站IP。

• 如果使用HTTPS,还需要准备服务器的证书和私钥。

6.1.2.2 添加防护域名

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到应用安全 > 域名配置, 如图 6-1: Web应用防火墙域名配置页面所示。

WAF的VIP为 10. 4,4	2. 0	
		请按照下列步骤添加您的域名 ^
* 域名:	<i>例</i> 妓I: www.aliyun.com	注意: 一级域名与二级域名需要分开配置
*协议类型:	П НТТР	
	HTTPS	
* 回源设置:		请以英文","隔开,不可换行,最多20个。
WAF是否支持XFF?:	◎ 是 ● 否 注意:若WAF前使用了七层代理,为了保障WAF的安全策略能够针对真	实源IP 生效,请务必选择"是"。
	确定 總已添加0个域名,还可以添加1000000个	

图 6-1: Web应用防火墙域名配置页面

3. 输入需要防护的域名,勾选协议类型,填写回源IP。

表 6-1: 域名配置项

	配置项	说明
ł	或名	支持配置泛域名,如*.aliyundemo.cn,可以匹配相关的二级域 名。当同时配置泛域名和精确域名时,转发和防护策略匹配顺 序以精确域名优先。

配置项	说明
协议	如果有HTTPS站点,务必勾选HTTPs协议类型。建议同时勾选 HTTP协议类型,以应对HTTP跳转等问题,保证访问平滑。
回源设置	回源IP是指希望Web应用防火墙把请求转发到的地址,一般是 真实服务器的地址(如ECS的IP),也可以是SLB的IP。 回源IP最多可以支持20个,Web应用防火墙支持负载均衡和健 康检查功能。
WAF是否支持XFF?	X-Forwarded-For位于HTTP协议的请求头, 是一个 HTTP 扩 展头部,用来表示 HTTP 请求端真实 IP。一般用于 HTTP 代 理、负载均衡等转发服务。 如果WAF前使用了七层代理,为了保障WAF的安全策略能够针 对真实源IP 生效,请务必选择 是 。

4. 单击**确定**。

6.1.2.3 上传HTTPS证书和私钥(仅针对HTTPS站点域名)

背景信息

如果需要防护HTTPS站点域名,必须将服务器的证书和私钥上传至Web应用防火墙,否则可能无法 正常访问HTTPS站点。

如果需要防护的域名不支持HTTPS协议访问,请跳过此步骤。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**。
- 3. 在协议类型中,勾选HTTPS。
- 4. 单击HTTPS高级设置可以选择HTTPS协议的回源方式及跳转设置,如图 6-2: HTTPS高级设置选项所示。

图 6-2: HTTPS高级设置选项

*协议类型:	HTTP
	✓ HTTPS 443
	HTTPS高级设置 ^
	开启HTTPS的强制跳转: (开启后,HTTP请求将显示为HTTPS,默认跳转到443端口)
	开启HTTP回源:
	示意图:
	HTTPS HTTP
	客户端浏览器 → WAF → 服务器

• 如果该站点不支持HTTPS回源,勾选**开启HTTP回源**,通过WAF实现HTTPS访问。使用该设置后,客户端可以通过HTTP和HTTPS方式访问站点。

送明:

使用HTTP回源,可以无需在源站服务器上做任何改动,也不需要配置HTTPS。但是,该配置的前提是在WAF上传正确的证书和私钥。

• 如果需要强制客户端使用HTTPS来访问,勾选**开启**HTTPS**的强制跳转**。

送 说明:

开启HTTPS强制跳转后,HTTP回源可以根据具体需求来开启或关闭。若同时开启HTTP回源,WAF会将客户端的HTTP请求重定向到HTTPS,并且设置客户端的HSTS属性(周期为一天)。支持HSTS的客户端后续会直接使用HTTPS访问,不支持的客户端则通过重定向方式访问。

5. 添加HTTPS站点域名后,在已添加域名列表中找到该域名,单击**上传证书**,如图 6-3: HTTPS站 点域名证书更新所示。

图 6-3: HTTPS站点域名证书更新

域名 ▼	请输入关键字进行域名模糊	查询	搜索				
-						ĺ	Ì
域名信息 站点IP: 编辑		业务状态 http https <mark>上传证书</mark> 编辑		安全状态 最近两天内无攻击	安全开关 Waf防护:防护 CC防护:正常 精准访问控制:开启 防护配置		

6. 上传服务器的证书文件和私钥文件,如图 6-4: 上传证书和私钥所示。

复制证书和私钥文本内容粘贴至相应的文本框内。

图 6-4: 上传证书和私钥

上传证书和私钥		×
当前域名的类型为HTT	「PS,需要进行证书和私钥导入才能正常防护网站。	
域名:	wwwcom	
证书文件 🕖 :		
私钥文件 🕖 :		
	确定	取消

一般如PEM、CER、CRT等证书格式,可用文本编辑器直接打开并复制内容;其它格式的证书(如PFX、P7B等)需要先转换成这些格式。如果有多个证书文件(如证书链),可拼接合并后一起上传。

• Web应用防火墙可识别的证书样例格式如下:

-----BEGIN CERTIFICATE---- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9f mxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2 cgHdj4v8H6jUz9Ji4mr7 vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc 65Cgb4mL+ n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKk vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== ----END CERTIFICATE----

• Web应用防火墙可识别的私钥样例格式如下:

-----BEGIN RSA PRIVATE KEY---- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn 2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQ Cr+ujntClkN6pGBj2Fw2l /EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYo aMF2EjRwc0 qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o 4Vqf0YF8bv5UK5G04RtKadOw== ----END RSA PRIVATE KEY----

7. 单击确定,完成配置。

6.1.2.4 放行Web应用防火墙VIP

背景信息

VIP是WAF用来代理客户端请求服务器时使用的源IP。在源站服务器看来,接入Web应用防火墙后 所有访问源IP都会变成Web应用防火墙的VIP,而真实的客户端地址会被加在HTTP头部的XFF字段 中。

域名接入Web应用防火墙后,需确保源站服务器的安全组已将Web应用防火墙的VIP放行,否则可能会出现网站无法访问或响应极其缓慢的情况。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**。
- 3. 在页面上方查看Web应用防火墙VIP,如图 6-5: Web应用防火墙VIP所示。

图 6-5: Web应用防火墙VIP



4. 登录Apsara Stack控制台,在源站服务器的安全组中将Web应用防火墙的VIP放行(在入方向,允许VIP访问源站服务器)。

安全组具体设置,参见《用户指南》的管理安全组。

6.1.2.5 本地验证域名Web应用防火墙接入配置

在把业务流量切到Web应用防火墙之前,建议先通过本地验证的方式确保配置正常,Web应用防火墙转发正常。

操作步骤

- 1. 登录云盾安全中心。
- 2. 在hosts文件中添加VIP和域名,使本地对于被防护站点的请求先经过Web应用防火墙。

以Windows 7为例修改hosts文件,文件路径C:\Windows\System32\drivers\etc\hosts

- a) 使用记事本等文本编辑器打开hosts文件。
- b) 在最后一行添加<WAF的VIP> <被防护域名>, 如图 6-6: Hosts文件添加内容示例所示内容。

图 6-6: Hosts文件添加内容示例



送 说明:

域名前面的IP为对应的Web应用防火墙所分配的VIP。

3. 在本地Ping被防护的域名,解析到的IP应该为在hosts文件中绑定的Web应用防火墙VIP。

说明:

如果依然解析到源站地址,可尝试刷新本地的DNS缓存。

4. 在浏览器中输入该域名进行访问。

如果Web应用防火墙的接入配置正确,则能够正常访问网站。

5. 验证Web应用防火墙保护功能。

例如,在域名的URL后添加/?alert(xss),即可模拟一个测试的Web攻击请求,如www. aliyundemo.cn/?alert(xss)。此时,Web应用防火墙应能弹出如图 6-7:Web应用防火墙 阻拦页面所示的阻拦页面。

图 6-7: Web应用防火墙阻拦页面



6.1.2.6 修改DNS解析

通过修改DNS解析到Web应用防火墙,完成业务正式接入。

背景信息

如果防护的站点域名不是通过域名解析服务商进行解析,例如站点是通过负载均衡(SLB)实例连接公网,也可以参考以下步骤,将所对应的SLB实例的回源IP修改为WAF的VIP,实现Web应用防火墙防护接入。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**。
- 3. 记录下Web应用防火墙为防护域名所分配的WAF的VIP。
- 4. 登录已防护站点的域名解析服务商所提供的控制台,定位到对应域名的域名解析设置,将A记录的值改为WAF的VIP。

送明:

域名解析的TTL值一般建议设置为600秒。TTL值越大,DNS记录的同步和更新越慢。

6.1.3 配置防护功能

在将站点接入Web应用防火墙防护后,可对所防护的站点进行详细的防护规则配置。

6.1.3.1 配置Web应用攻击防护

启用Web应用攻击保护功能,并设置防护模式和防护规则。

背景信息

Web应用攻击防护功能可以防护SQL注入、XSS跨站脚本、文件上传、文件包含、常见目录遍历、 常见CMS漏洞、代码执行注入、脚本后门攻击、扫描器攻击等常见Web应用攻击。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**页面。
- 3. 选择已接入Web应用防火墙进行防护的站点域名,单击**防护配置**,如图 6-8: 域名防护配置所示。

图 6-8: 域名防护配置

域名 ▼ 请输入关键字进行域	洺模糊查询 搜索			
www.				â
域名信息 站点IP: 编辑	业务状态 http https 上传证书 编辑	安全状态 最近两天内无攻击	安全开关 Waf防护:防护 CC防护:正常 藏 進访问控制:开启 防护配置	

- 4. 定位到web应用攻击防护功能项,单击状态栏后的启用按钮并选择防护模式及防护规则策
 - 略,如图 6-9: Web应用攻击防护功能项所示。
 - 图 6-9: Web应用攻击防护功能项

‡ D	
	模式: 💿 防护 🔘 预警 🕧
防护SQL注入、XSS跨站等常见Web应用攻击、实时生效。	防护规则策略:正常 🔻 🕖

表 6-2: 防护模式和防护策略

防护设置		说明	
防护模式	防护	Web应用防火墙自动对攻击行为进行阻断。	
	预警	Web应用防火墙对可疑攻击告警但不立刻阻断,方便 评估误报情况。	
防护规则策略	正常	默认策略,一般情况下使用。	
	宽松	当发现正常模式规则存在较多误拦截的情况,或业务 存在较多不可控的用户输入(例如富文本编辑器、技 术论坛)时,建议选择宽松模式。	
	严格	需要更严格的防护规则来防护路径穿越、SQL注入、 命令执行等攻击,建议选择严格模式。	

6.1.3.2 配置恶意IP惩罚

当某个IP在短时间内进行多次Web攻击,可以设置自动封禁该IP一段时间。

前提条件

只有同时启用Web应用攻击防护和CC安全防护后,才能启用恶意IP惩罚。

背景信息

传统的Web应用防火墙产品,基本都是针对 IP-URL 维度的拦截。当判定一个请求是攻击行为

后,仅仅把这个请求进行单次阻断。而实际上,恶意攻击者们日复一日地在对用户的网站进行扫

描、攻击,黑客可能一个通宵都在挖掘网站的漏洞,研究防护策略并尝试绕过。

专有云云盾Web应用防火墙提供了恶意IP惩罚功能。利用阿里云平台积累的海量恶意IP库和机器学 习功能,对发起攻击行为的 IP、攻击频率进行学习分析,自动生成判定规则。当发起攻击的IP的行 为被判定为持续攻击行为,Web应用防火墙将直接阻断这个IP的所有访问请求。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**页面。
- 3. 选择已接入Web应用防火墙进行防护的域名,单击防护配置。
- 4. 定位到恶意IP惩罚功能项,单击状态栏后的启用按钮即可启用恶意IP惩罚功能,如图 6-10:恶意IP惩罚功能项所示。

图 6-10: 恶意IP惩罚功能项



6.1.3.3 配置CC安全防护

通过独家算法防护引擎并结合大数据,拦截CC攻击。

背景信息

CC(Challenge Collapsar)攻击,是一种专门针对于Web的应用层FLOOD攻击,是DDoS的一

种。攻击者通过代理服务器或者肉鸡,对目标Web服务器进行海量http request攻击,造成对方服务 器资源耗尽。

Web应用防火墙提供了正常、攻击紧急两种CC安全防护模式:

- **正常**:CC安全防护的默认模式,只会针对特别异常的请求进行拦截,误杀可能性较小。
- **攻击紧急**:攻击紧急模式拦截CC攻击效果较强,但可能存在误杀的情况。当发现站点遭受CC攻击,且正常模式无法有效拦截时,可以启用攻击紧急模式。

攻击紧急模式仅适用于普通网页及HTML5页面,对于API、Native APP的业务可能会造成大量 误杀。如果需要为API、Native APP业务配置CC攻击防护,请使用CC自定义规则进行防护。

同时,Web应用防火墙提供了CC防护自定义规则,支持在控制台自定义对于特定URL路径的访问频率限制。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**页面。
- 3. 选择已接入Web应用防火墙进行防护的域名,单击**防护配置**。
- 定位到cc安全防护功能项,单击状态栏后的启用按钮,选择想要应用的CC安全防护模式,如图
 6-11: CC安全防护功能项所示。

图 6-11: CC安全防护功能项



5. 单击自定义规则栏后的启用按钮,可启用CC安全防护自定义规则。

自定义规则设置如下:

a) 单击前去配置, 配置自定义防护规则, 如图 6-12: CC自定义安全防护规则所示。

图 6-12: CC自定义安全防护规则

CC攻击自定义规则 總还可以添加 19 条 新機規則						王可以添加19条 新增规则	
规则名称	URL	检测时长	单一IP访问次数	匹配规则	阻断类型	时长	操作
111	/111	5	2	前缀匹配	封禁	10分钟	編載 删除

b) 单击**新增规则**, 添加想要设置的自定义规则。

例如,通过自定义防护规则可设置当单个访问源IP在10秒内访问www.abc.com/login.html超过20次,即封禁该IP一小时。

图 6-13: 新增自定义规则

新增规则		×
规则名称	Demo	
URI :	/login.html	
匹配规则	💽 完全匹配 🔘 前缀匹配	
检测时长:	10 秒	
单一IP访问次数:	20 次	
阻断类型	● 封禁 ○ 人机识别	
	60 分钟	
	確	定取消

表 6-3: 规则参数说明

规则参数	说明
URI	需要防护的具体URI地址,如/register。同时,支持输入参数,如/user?action=login。
匹配规则	 完全匹配:即精确匹配,请求必须跟所配置的URI完全一致才适用该规则。 前缀匹配:指包含匹配,只要是请求的URI以配置的URI地址开头都适用该规则,如/register.html。
检测时长	访问次数的周期时长,与单一IP访问次数配置相配合。
单一IP访问次数	在统计周期内,单个源IP访问该URL的次数。
阻断类型	 • 封禁:触发规则条件后,直接断开连接。 • 人机识别:触发规则条件后,通过重定向的方式进行客户端人机识别,成功通过验证的请求才可放行。

规则参数	说明
阻断时间	执行阻断动作的时间。

c) 单击确定。

6.1.3.4 配置精准访问控制

精准访问控制功能支持针对常见的HTTP字段(如IP、URL、Referer、UA、参数等)进行条件组合设置访问控制规则,支持业务场景的定制化防护策略,如盗链防护、网站管理后台保护等场景。

背景信息

配置精准访问控制规则之前,请注意以下事项:

- 每一条规则中最多允许由三个条件组合。
- 同一条规则中的多个条件之间都是"与"的逻辑关系,即必须同时满足多个条件才算匹配中规则。
- 匹配中规则后可设定的匹配动作有三种:
 - 阻断:阻止访问。
 - 放行:选择放行后,可选择后续是否继续执行Web应用攻击防护或CC攻击防护。
 - 告警:只记录不阻断。
- 精准访问控制规则之间存在先后匹配顺序,可通过调整规则排序达到最优的防护效果。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**页面。
- 3. 选择已接入Web应用防火墙进行防护的域名,单击**防护配置**。
- 2. 定位到精准访问控制功能项,单击状态栏后的启用按钮即启用精准访问控制功能,如图 6-14:精 准访问控制功能项所示。

图 6-14: 精准访问控制功能项



5. 单击前去配置,配置精准访问控制规则,如图 6-15: 配置精准访问控制规则所示。

图 6-15: 配置精准访问控制规则

	度:当前每一多规则中最多九许三个条件组合,并且条件之间是"与"的逻辑关系(<mark>即必须三个条件同时满足才算匹配中规则),</mark> 匹配中规则后的动作有三种:组断、放行(可 <mark>说将后续是否继续进行Web攻击拦截或CC攻击</mark>)、告警(只记录不阻断), 则之间是有先后匹面顺序的,可点击 <mark>规则排序</mark> 达到最优的防护效果。					
l	精准访问控制				您还可以添加 100 条	新增规则规则排序
l	规则名称	规则条件	动作	后续安全策略		操作
	聚代认 规则	所有请求	放行	Web通用防护 ⊘ CC防护 ⊘		SRSR
					共有1条 ,每页显示:10条	« c 1 > »

6. 单击新增规则,如图 6-16:新增精准访问控制规则所示。

图 6-16: 新增精准访问控制规则

新增规则			×
规则名称 : 匹配条件 :	test		
匹配字段	逻辑符	匹配内容	
URL V URL IP Referer User-Ager Params 匹配动作:	包含 v nt	只允许填写一个匹配项,暂不支持正则,不填代	末 空 ×
			确定取消

匹配字段	说明
IP	访问请求的来源IP。
URL	访问请求的URL地址。
Referer	访问请求的来源网址,即该访问请求是从哪个页面跳转产生的。
User-Agent	发起访问请求的客户端的浏览器标识、渲染引擎标识和版本信 息等浏览器相关信息。
Params	访问请求的URL地址中的参数部分,通常指URL中问 号(?)后面的部分。

精准访问控制规则支持多种匹配字段及逻辑符,可根据实际业务需求进行规则设置,也可以参考 如图 6-17:精准访问控制规则样例所示的规则样例设置匹配规则。

图 6-17: 精准访问控制规则样例

1					
精准访问控制			您还可以添加 193 条 新	[」]	序
规则名称	规则条件	动作	后续安全策略	ł	操作
	请求URL 等于 /user				
只允许通过微信登录	请求Params 包含 action=login	阻断		编辑:	删除
	请求User-Agent 不包含 MicroMessenger				
只允许公司访问后台	请求IP 不属于 1.2.3.0/29	阳新		2日	₩6¢
	请求URL 包含 admin.php	PELOT		403-044-0	Ranas
防WP攻击	请求User-Agent 包含 wordpress	阻断		编辑:	删除
『古ンのおね	请求URL 包含 photos	阳城		台場	an ræ
WJ mm trz	请求Referer 包含 blog.xxxx.com	(<u>H</u> u)		509468 S	1011101
黑名单1	请求IP 雇于 4.4.4.0/24	阻断		编辑	删除
白名单2	请求IP	放行	Web通用防护 🥝	编辑	删除
白名单1	请求IP	放行		编辑:	删除
默认规则	所有未命中以上规则的请求	放行	Webi通用防护 🔮 CC防护 🥝	ŧ	编辑

7. 在**精准访问控制**页面,单击规则排序可对已设定的精准访问控制规则进行排序,调整完成后单击保存即可。精准访问控制功能将按设置的规则顺序进行匹配。

6.1.3.5 配置封禁地区

Web应用防火墙可对特定地区的来源IP进行封禁。根据IP归属地信息库,封禁地区功能针对支持国内各省份和海外地区的IP封禁。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 域名配置**页面。
- 3. 选择已接入Web应用防火墙进行防护的域名,单击防护配置。
- 2. 定位到封禁地区功能项,单击状态栏后的启用按钮即启用封禁地区功能,如图 6-18: 封禁地区功 能项所示。

图 6-18: 封禁地区功能项



5. 单击设置,可对封禁的地区进行设置,如图 6-19: 设置封禁地区所示。

图 6-19: 设置封禁地区

选择	泽地区							×
请说 全议	先择您要封禁 先	的地区:						
-	上海市	云南省	内蒙古自	治区は	「京市	台湾省	海外	
	吉林省	四川省	天津市	宁夏回放	<u> 全自治区</u>	安徽省		
	山东省	山西省	广东省	广西壮油	<u> 全自治区</u>			
	新疆维吾	尔自治区	江苏省	江西省	河北省	i -		
	河南省	浙江省	海南省	湖北省	湖南省	li -		
	澳门特别	行政区	甘肃省	福建省	西藏自治			
	贵州省	辽宁省	重庆市	陕西省	青海省	i i		
	香港特别	行政区	黑龙江省					
							确定	取消

6.1.4 查看安全报表

Web应用防火墙提供了各种安全报表供安全管理员实时了解所防护的域名的安全状态。

6.1.4.1 查看安全总览

展示攻击防护报表和Web防护规则相关消息。

背景信息

WEB攻防总览页面展示了攻击防护报表和Web防护规则相关消息。

- 在攻击防护报表中,可以查看Web攻击、CC攻击的防护情况,并显示昨日、今日及30天内防护 次数,帮助安全管理员快速了解所防护的域名的整体安全状态。
- 在消息区域中,可以查看阿里云实时发布的Web应用防火墙防护规则的更新消息。

操作步骤

1. 登录云盾安全中心。

- 2. 定位到应用安全 > WEB攻防总览。
- 3. 查看Web应用防火墙攻击防护信息,如图 6-20:安全总览页面所示。

图 6-20: 安全总览页面

安全总览					
↓攻击防护					消息
Web攻击					
4.0k					
2.0k					() 暂无数据,敬请期待!
0	40.00	10.15	40.00		
	昨日22:0	10-15 今日: 0	10-22 30天: 421 9	10-29	

单击攻击防护报表右上方的查看详情按钮,跳转至WEB安全报表页面,查看详细攻击防护情况。

6.1.4.2 查看安全报表

查看Web应用防火墙所防护的域名的详细防护情况。

背景信息

在WEB安全报表页面,可查看Web应用防火墙所防护的域名的详细防护情况。

- 针对Web应用攻击,可以查看攻击类型分布、攻击来源IP、攻击来源区域及详细的攻击记录。
- 针对**CC攻击**,可以查看服务器每秒查询率(QPS),包括总QPS、攻击QPS信息及详细的恶意CC攻击事件记录。
- 针对访问控制事件,可以查看已配置的精准访问控制规则的匹配次数及对应的规则动作。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > WEB安全报表**页面。
- 3. 查看Web应用攻击安全报表。
 - a) 单击Web应用攻击,并设置域名和查询时间,如图 6-21: Web应用攻击安全报表所示。

图 6-21: Web应用攻击安全报表

安全服表				
 				
安全攻击类型分布	攻击来源IP TOP5		攻击来源区域 TOP5 (溃后一天)	
	10. (未分配或者内网	3219 次	未有来源区城	
	10 末分配或者内网1	1000 次	未有来源区域	
	未有访问IP		未有来源区域	
	末育访问IP		未有來源区域	
	未有访问IP		未有未源区域	
● SQL注入				
攻击中	所雇地区	最后一次攻击时间♦	总攻击次数单	1荣行=
10	未分配或者内网IP	2017-10-27 16:09:27.0	3219	查看攻击详情
10	未分配或者内网IP	2017-10-27 08:59:05.0	1000	查看攻击详情
			共有2条 ,每页显示:10条	« (<mark>1</mark>) »

b) 单击**查看攻击详情**,可查看详细的攻击事件及所触发的拦截规则,如图 6-22: 查看攻击详 情所示。

图 6-22: 查看攻击详情

查看攻击详情						×
2017-10-27						
攻击时间	攻击URL	攻击类型(全部) ▼	规则描述	请求方 法	请求参 数	规则动 作
2017-10-27 1 6:09: 27	www	SQL注入	SQL注入防护规则(and/or特 征)	GET		阻断
2017-10-27 16:09: 27	wwwcom/and	SQL注入	SQL注入防护规则(and/or特 征)	GET		阻断
2017-10-27 1 6:09: 26	wwwcom/and	SQL注入	SQL注入防护规则(and/or特 征)	GET		阻断
2017-10-27 16:09: 24	wwwcom/and	SQL注入	SQL注入防护规则(and/or特 征)	GET		阻断
2017-10-27 16:08: 14	wwwcom/and	SQL注入	SQL注入防护规则(and/or特 征)	GET		阻断
		共有3219	9条 , 每页显示 : 5条 《	< 1	2 3	> >>
						关闭

4. 查看CC攻击安全报表,如图 6-23: CC攻击安全报表所示。

图 6-23: CC攻击安全报表

安全报表 															
爭城名:	www	com ¢	查询时间:	昨天 今	天 7天	30天	法则日期可精准的	胚沟							
60															
50															
40															
30															
20															
10															
0	10-03	10-05	10-07	10-09	10-11	10-13	10-15	10-17	10-19	10-21	10-23	10-25	10-27	10-29	10-31 11-01
意 定 C 攻	女击事件 (事)	件定义:攻击持	续时间 > 3分钟	目每秒攻击次费	(> 100)										
(由时间)											攻击次数			QPS線值	
17-10-30	0 17:32:00 至	2017-10-30 17	:45:00								415			101	
												共有	11条,每页显	示:10条 《	< 1 >

5. 查看访问控制事件安全报表,如图 6-24: 访问控制事件安全报表所示。

图 6-24: 访问控制事件安全报表

选择类型:	Web应用攻击 CC攻击	访问控制事件			
选择域名:	全部 ◆ 查询时间:	昨天 今天 7天	30天		
规则ID		规则描述		匹配次数	规则动作
114		默认规则		10	放行
125				10	
116		规则1		10	阻断

6.1.4.3 查看业务分析

业务分析功能结合Web应用防火墙的攻击拦截情况及访问流量,通过大数据引擎,对所防护域名的 业务访问情况进行分析,帮助安全管理员及时发现业务漏洞,提升防御能力。

前提条件

Web应用防火墙的业务分析功能依赖于MaxCompute(原名 ODPS)服务进行数据分析。如果专有 云环境中没有部署MaxCompute产品,将无法使用业务分析功能。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**应用安全 > 业务分析**页面。
- 3. 选择域名及查询时间,查看业务分析结果,如图 6-25: 业务分析页面所示。

图 6-25: 业务分析页面

业务分析		
选择域名: www.example.com 🔻 查询时间: 昨天	今天 7天 30天	
访问次数	访问IP数	
	暂无查询数据	暂无查问数据
昨日: 0 次 今日: 0 次	30天: 0 次	昨日: 0 IP 今日: 0 IP 30天: 0 IP
响应时间TOP5	访问IP次数TOP5	请求来源区域TOP5
未有访问网址	未有访问IP	未有来源区域
未有访问网址	未有访问IP	未有来源区域
未有访问网址	未有访问IP	未有来源区域
未有访问网址	未有访问IP	未有來源区域
未有访问网址	未有访问IP	未有來源区域
服务器响应状态	访问流量的	刘览器分布
	智无查询数据	智无查询数据

7 云主机安全

7.1 主机安全总览

主机安全总览对云主机整体安全情况进行概要性展示,以便安全管理员快速了解和掌握当前安全情况。

主机安全总览包括总览、弱点、事件、ECS保护状态、最近重要弱点和事件。

总览

整体展现云主机环境各类型的安全弱点(待处理漏洞、基线配置不当)和安全事件(异常登录、网站后门、主机异常)的数量。

总览			
103 个 ^{属两待处理}	21 ↑ ^{异常登录}		Ţ

弱点

展示云主机存在的安全弱点趋势。安全弱点如果不修复,存在安全隐患,具体修复建议和操作可以参考安全预防。



- 上面为过滤条件,通过类型、严重程度和展示时间,生成展示结果。
- 左侧为弱点发现趋势,展示一段时间内云主机的弱点趋势。
- 右侧为TOP弱点主机,展示存在弱点数量最多的云主机。

事件

展示云主机存在的安全事件趋势。安全事件表明目前云主机已经发现的安全入侵行为,具体操作可以参考入侵检测。



- 上面为过滤条件,通过类型、严重程度和展示时间,生成展示结果。
- 左侧为入侵事件趋势,展示一段时间内云主机受到入侵的趋势。
- 右侧为TOP安全事件主机,展示受到入侵最多的云主机。

ECS保护

查看目前云主机中正在受到保护的主机数量和离线数量。



最近重要弱点和事件

展示最近重要的云主机安全弱点和安全事件,单击连接可以查看具体详细情况。

最近重要弱点和事件

【未修复】2018-06-02 05:11:49 【192.168.77.18(iZ5wf05ykw7minn5ge2ma9Z)】 漏洞: RHSA-2017:0252: ntp security update

【未修复】2018-06-02 05:11:49 【192.168.77.18(iZ5wf05ykw7minn5ge2ma9Z)】 漏洞: RHSA-2017:1574: sudo security update

【未修复】2018-06-02 05:11:49 【192.168.77.18(iZ5wf05ykw7minn5ge2ma9Z)】 漏洞: RHSA-2016:2824: expat security update

7.2 主机列表

以云主机维度,展示各主机的安全状况信息。

7.2.1 管理主机列表

在主机列表页面,可以查看安骑士已防护的服务器的状态。

背景信息

服务器保护状态分为在线、离线、暂停保护三种。

- 在线:安骑士为该服务器提供全面的安全防护。
- 离线:安骑士服务端无法与该服务器的客户端正常连通,无法提供安全防护功能。
- 暂停保护:暂时关闭安骑士对该服务器的防护,具体参见暂停保护操作。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 主机列表。
- 3. (可选)搜索服务器。

如果想查看某台服务器的安全状态,也可以在搜索框中输入该服务器的IP,并单击**搜索**,即可快 速查看该服务器的详细信息和安全信息。

4. 查看服务器的保护状态和具体安全信息。

单击右上角的 🐢 , 设置服务器具体显示哪些信息列。信息主要分为以下几类。

类别	信息
服务器基本信息	• 服务器IP/名称

类别	信息
	 标签 操作系统
	• 地域
保护状态	保护状态
安全预防	 漏洞 基线
入侵检测	 ・ 异常登录 ・ 网站后门 ・ 主机异常
主机指纹	 ・ 进程数 ・ 端口数 ・ Root账号/所有账号

5. 管理服务器。

功能	操作说明
更改分组	勾选服务器,单击 更改分组 ,更改服务器所在的分组。分组具体说 明参见 <mark>管理</mark> 分组。
设置标签	勾选服务器,单击 设置标签 ,设置服务器标签信息。
一键安全检查	勾选服务器,单击 一键安全检查 ,可以选择从多维度对服务器进行 安全检查。
删除非阿里云机器	勾选 非阿里云 的服务器,单击 更多操作 > 删除非阿里云机器 。
暂停保护	勾选 在线 状态的服务器,单击 更多操作 > 暂停保护 ,暂时关闭安骑 士对该服务器的防护,降低该服务器的资源消耗。
开启保护	勾选 暂停保护 状态的服务器,单击 更多操作 > 开启保护 ,开启安骑 士对该服务器的防护。

7.2.2 管理分组

为了方便对特定服务器进行安全管控,可以对服务器进行分组,通过分组的维度查看安全事件。

背景信息

未进行分组时,所有的服务器都在**未分组**中。当您删除某个分组时,该分组中的服务器也将默认移入**未分组**中。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**云主机安全 > 主机列表**。
- 3. 管理子分组。

分组排序	
所有资源 115台	
- 🕀 未分组 99台	
\oplus	
── 测试分组 1台	
- 🕀 基线检查分组 1台	$+ \times \checkmark$

• 新建子分组。

单击所有资源或者子分组右侧的添加按钮,输入子分组名称并单击确认。

说明:

最多支持三级子分组。

• 修改子分组。

单击子分组右侧的修改按钮,输入子分组名称并单击确认。

• 删除子分组。

单击子分组右侧的删除按钮,在弹出的确认框中单击确认。



删除后该分组中的服务器默认移入未分组。

- 4. 给服务器进行分组。
 - a) 在右侧的服务器列表中, 勾选服务器。
 - b) 单击**更换分组**。
 - c) 在弹出窗口的下拉菜单中选择分组。
 - d) 单击**确认**。
- 5. 切换分组排序。

单击**分组排序**,可以把优先级高的分组移动到上面。

7.3 安全预防

安全预防提供漏洞管理和基线检查功能,用于发现服务器中存在的漏洞和风险点,并提供修复建议。

7.3.1 漏洞管理

漏洞管理扫描出服务器中存在的漏洞,并提供漏洞修复方法。

7.3.1.1 管理Linux软件漏洞

比对CVE官方漏洞库,自动检测您服务器上安装的软件版本是否存在漏洞,并向您推送漏洞消息。 针对检测到的漏洞,提供漏洞修复指令和验证功能。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 漏洞管理,选择Linux软件漏洞页签。
- 3. 查看所有漏洞。

通过漏洞搜索和筛选功能,快速定位到具体漏洞,如图 7-1:过滤漏洞所示。

图 7-1: 过滤漏洞

漏洞搜索:	请输入漏洞名	称			搜索
是否已处理	: 未处理	已处理			
修复紧急度	: 全部	需尽快的	复		
漏洞等级:	严重	高危	中危	低危	

单击漏洞名称,进入漏洞详情页,查看漏洞详细信息和影响资产。
 通过搜索和筛选功能,快速展示影响资产,如图 7-2:筛选影响资产所示。
图 7-2: 筛选影响资产

影响资产			
资产选择: 所有分组 🔹	服务器IP或名称	服务器标签	搜索
是否已处理: 未处理 E	己处理		
修复必要性: 需尽快修复	可延后修复 暂可不修复		

5. 根据漏洞影响情况,选择相应的处理方式,如表 7-1:漏洞操作方式所示。

表 7-1: 漏洞操作方式

操作	说明
生成修复命令	自动生成修复漏洞的指令,然后登录服务器运行该指令来修复漏洞。
一键修复	直接修复漏洞。
已重启并验证	如果修复漏洞需要重启服务器才能生效,必须等待漏洞修复状态变为 修复 成功待重启后,重启该服务器,然后单击已重启并验证完成修复。
忽略	可忽略该漏洞,系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后,单击 验证 ,一键验证该漏洞是否已修复成功。 如果未进行手动验证,漏洞修复成功后 48 小时内系统会自动去验证。

对于影响资产,可以进行单个操作或多个批量操作。

- 单个操作:在操作列,对单个受影响的服务器进行处理。
- 批量操作:勾选一个或多个需要处理的服务器,使用列表下方的批量操作按钮进行批量处理。

7.3.1.2 管理Windows系统漏洞

比对微软官方补丁更新,自动检测您服务器上的补丁是否已更新,并向您推送漏洞消息。针对重大漏洞更新,提供自动检测和修复功能。

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 漏洞管理,选择Windows系统漏洞页签。
- 3. 查看所有漏洞。

通过漏洞搜索和筛选功能,快速定位到具体漏洞,如图 7-3:过滤漏洞所示。

图 7-3: 过滤漏洞

漏洞搜索: 请输入漏洞名称	搜索
是否已处理: 未处理 已处理	
修复紧急度:全部需尽快修复	
漏洞等级: 严重 高危 中危 低危	

4. 单击漏洞名称,进入漏洞详情页,查看漏洞详细信息和影响资产。

通过搜索和筛选功能,快速展示影响资产,如图 7-4: 筛选影响资产所示。

图 7-4: 筛选影响资产

影响资产		
资产选择: 所有分组 ▼ 服务器IP或名称	服务器标签	搜索
是否已处理: 未处理 已处理		
修复必要性: 需尽快修复 可延后修复 暂可不修复		

5. 根据漏洞影响情况,选择相应的处理方式,如表 7-2:漏洞操作方式所示。

表 7-2: 漏洞操作方式

操作	说明
立即修复	直接修复漏洞。系统会在云端缓存一份Windows官方补丁文件,您的 Windows系统服务器会直接下载云端的补丁并完成自动更新。
忽略	可忽略该漏洞,系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后,单击 验证 ,一键验证该漏洞是否已修复成功。
已重启并验证	如果修复漏洞需要重启服务器才能生效,必须等待漏洞修复状态变为 修复 成功待重启后,重启该服务器,然后单击已重启并验证完成修复。

对于影响资产,可以进行单个操作或多个批量操作。

- 单个操作:在操作列,对单个受影响的服务器进行处理。
- 批量操作:勾选一个或多个需要处理的服务器,使用列表下方的批量操作按钮进行批量处理。

7.3.1.3 管理Web-CMS漏洞

Web-CMS 漏洞功能通过及时获取最新的漏洞预警和相关补丁,并通过云端下发补丁更新,实现漏 洞快速发现、快速修复的功能。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 漏洞管理,选择Web-CMS漏洞页签。
- 3. 查看所有漏洞。

通过漏洞搜索和筛选功能,快速定位到具体漏洞,如图 7-5:过滤漏洞所示。

图 7-5: 过滤漏洞

漏洞搜索: 请输入漏洞名称	搜索
是否已处理: 未处理 已处理	
修复紧急度:全部零尽快修复	
漏洞等级: 严重 高危 中危 低危	

4. 单击漏洞名称,进入漏洞详情页,查看漏洞详细信息和影响资产。

通过搜索和筛选功能,快速展示影响资产,如图 7-6:筛选影响资产所示。

图 7-6: 筛选影响资产

影响资产		
资产选择: 所有分组 ▼ 服务器IP或名称	服务器标签	搜索
是否已处理:未处理 已处理		
修复必要性: 需尽快修复 可延后修复 暂可不修复		

5. 根据漏洞影响情况,选择相应的处理方式,如表 7-3:漏洞操作方式所示。

表 7-3: 漏洞操作方式

操作	说明
立即修复	系统将替换服务器上存在漏洞的Web文件以修复Web-CMS漏洞。
	说明 : 修复Web-CMS漏洞前,建议备份该漏洞相关的Web文件,Web文件的 具体路径可参考漏洞处理说明栏中的路径。
忽略	可忽略该漏洞,系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后,单击 验证 ,一键验证该漏洞是否已修复成功。 如果未进行手动验证,漏洞修复成功后 48 小时内系统会自动去验证。
回滚	对于已修复完成的漏洞,单击 回滚 可进行漏洞回滚,还原修复前的Web文件。

对于影响资产,可以进行单个操作或多个批量操作。

- 单个操作:在操作列,对单个受影响的服务器进行处理。
- 批量操作:勾选一个或多个需要处理的服务器,使用列表下方的批量操作按钮进行批量处理。

7.3.1.4 管理其他漏洞

自动检测服务器上的Redis未授权访问漏洞、STRUTS-052命令执行漏洞等漏洞,并推送漏洞消息。同时,支持漏洞的修复验证操作。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 漏洞管理,选择其他漏洞页签。
- 3. 查看所有漏洞。

通过漏洞搜索和筛选功能,快速定位到具体漏洞,如图 7-7:过滤漏洞所示。

图 7-7: 过滤漏洞

漏洞搜索:	请输入漏洞名称			搜索	
是否已处理	: 未处理	已处理			
修复紧急度	: 全部	需尽快的	复		
漏洞等级:	严重	高危	中危	低危	

单击漏洞名称,进入漏洞详情页,查看漏洞详细信息和影响资产。
 通过搜索和筛选功能,快速展示影响资产,如图 7-8: 筛选影响资产所示。

图 7-8: 筛选影响资产

影响资产		
资产选择: 所有分组 ▼ 服务器IP或名称	服务器标签	搜索
是否已处理: 未处理 已处理		
修复必要性: 需尽快修复 可延后修复 暂可不修复		

5. 根据漏洞影响情况,选择相应的处理方式,如表 7-4:漏洞操作方式所示。

其他漏洞需要按照修复说明手动修复。

表 7-4: 漏洞操作方式

操作	说明
忽略	可忽略该漏洞,系统将不再上报并告警此服务器上被忽略的漏洞。
验证	手动修复漏洞后,单击 验证 ,一键验证该漏洞是否已修复成功。 如果未进行手动验证,漏洞修复成功后 48 小时内系统会自动去验证。

对于影响资产,可以进行单个操作或多个批量操作。

- 单个操作:在操作列,对单个受影响的服务器进行处理。
- 批量操作:勾选一个或多个需要处理的服务器,使用列表下方的批量操作按钮进行批量处理。

7.3.1.5 设置漏洞管理策略

漏洞管理设置允许您开启/关闭不同类型漏洞的自动检测,有选择性地对指定服务器应用漏洞检测,对已失效漏洞设置自动删除周期,和配置漏洞白名单。

背景信息

漏洞白名单用于彻底忽略某些漏洞,您可以在漏洞列表下批量添加漏洞至白名单。添加成功后,系统将不再去检测漏洞白名单中的漏洞。使用漏洞管理设置可以维护漏洞白名单。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 漏洞管理。
- 3. 单击右上角的漏洞管理设置,配置相关策略,如图 7-9: 漏洞管理设置所示。

图 7-9: 漏洞管理设置

漏洞管理设置	\times
Linux软件漏洞: 共116台(已全部开启) 管理	
Windows漏洞: 共116台(已全部开启) 管理	
Web-CMS漏洞: 共116台(还有104台未开启) 管理	
其他漏洞: 👥 🚺 共116台(还有1台末开启) 管理	
扫描漏洞等级范围: ✓ 严重 □ 高危 □ 中危 □ 低危 失效漏洞自动删除: 7天 ▼ 漏洞白名单配置:	
□ 漏洞名称	操作
 Microsoft.NET Framework安全更新 	移除
RHSA-2017:1842: kernel security, bug fix, and enhancement update (Important)	移除

• 选择需要操作的漏洞类型,单击切换开关,开启/关闭该漏洞检测。

- 选择需要操作的漏洞类型,单击管理,配置应用该漏洞检测的服务器。
- 勾选需要扫描的漏洞等级:严重、高危、中危、低危。
- 选择失效漏洞自动删除周期:7天、30天、90天。



对于检测出来的漏洞不做任何处理的话,默认该告警失效,并在指定周期后自动删除。

• 在漏洞白名单下勾选相应漏洞,单击移除,重新启用对该漏洞的检测和告警。

7.3.2 基线检查

检测服务器上的系统、数据库、账号配置存在的风险点,并针对所发现的问题项提供修复建议。

7.3.2.1 基线检查介绍

安骑士基线检查功能自动检测服务器上的系统、数据库、账号配置存在的风险点,并针对所发现的 问题项提供修复建议。

检测原理

基线检查功能自动检测服务器上的系统、权限、账号、数据库等配置存在的风险点,并提供修复建议。

检测周期

默认每三天进行一次全面自动检测,自动检测在凌晨0到6点间完成。您可以在在安全设置页面设置 检测周期和检测发生时间。

注意事项

某些检测项,例如:Mysql弱密码检测、sqlserver弱密码检测,会采用尝试登录方式进行检查,会 占用一定的服务器资源以及生产较多的登录失败记录,这些项目是默认不开启的。如果需要这些功 能,请确认上述风险后,在基线检查设置中勾选这些项目。

检测内容

表 7-5: 检测内容

分类	检测项
CIS基线检测	Centos7基线检测
	Tomcat7基线检测
弱密码检测	PostgreSQL弱密码检测

分类	检测项
	SSH弱密码检测
	FTP匿名登录检测
	SQLServer登录密码检测
	MySQL弱密码检测
	RDP弱密码检测
	FTP弱密码检测
系统	组策略
	文件监控
	基线策略
	注册表
账号	系统账号安全
数据库	Redis合规检查

7.3.2.2 管理基线检查

通过基线检查功能,查看和修复服务器上的配置风险项。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 基线检查,进入基线检查页面。
- 3. 查看所有风险项。

通过风险搜索和筛选功能,快速定位到具体风险。

风险搜索:请输入风险	名称		搜	索	
是否已处理: 未处理	已处理				
风险分类: 全部	cis	弱密码检测	系统	账号	数据库
风险等级:严重	高危	中危	低危		

4. 单击风险名称,可查看该风险详情及相关修复建议。

加入白名单:如果发现风险对服务器没有影响,后续也不需要检查该风险,可以单击右上角的加入白名单。

- 5. 参考修复建议,在您的对应服务器上进行修复。
 - 修复风险后,您可以单击验证,一键验证该风险是否已修复成功。如果您未进行手动验证,风险修复成功后 72 小时内安骑士会进行自动验证。
 - 如果不需要修复,您可以单击**忽略**,忽略该风险,安骑士将不再上报并告警此服务器上的这个风险项。

7.3.2.3 设置基线检查策略

根据实际业务情况设置基线检测项,检测周期、检测风险等级。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 安全预防 > 基线检查,进入基线检查页面。
- 3. 单击基线检查设置,可以新建或者修改策略。
- 4. 单击添加,配置策略。

选择某一策略,单击编辑修改策略;单击删除删除策略。

5. 管理白名单。

7.4 入侵检测

入侵检测提供异常登录、网站后门和主机异常等功能,用于检测发现服务器受到的入侵行为。

7.4.1 异常登录

在安骑士管理控制台中的**异常登录**页面,您可以查看服务器上每次登录行为有异常的登录IP、账号、时间,包括异地登录告警及非法登录IP、非法登录时间、非法登录账号的登录行为告警。 安骑士Agent通过定时收集您服务器上的登录日志并上传到安骑士服务器端,在安骑士服务器端进

行分析和匹配。如果发现在非常用登录地或非法登录IP、非法登录时间、非法登录账号的登录成功 事件,将会触发事件告警。

异地登录告警策略如图 7-10: 异地登录策略所示。

图 7-10: 异地登录策略



短信告警方式:可以在**设置 > 告警配置**中,选择**登录安全 > 异常登录**通知项目的告警方式(可配 置为短信、邮件、及站内信方式,默认通过全部方式进行告警)。

针对机器设置合法登录IP、合法登录时间、合法登录账号,在上述合法登录IP、合法登录事件、合法登录账号之外的登录行为均提供告警,判断优先级高于异地登录判断。

7.4.1.1 查看异常登录

查看异常登录告警,包括异地登录、爆破登录、非法IP登录、非法账号登录和非法时间登录等告 警。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 入侵检测 > 异常登录。
- 3. 查看所有异常登录信息。

通过搜索和筛选功能,快速定位到具体异常登录信息,如图 7-11:查找异常登录信息所示。

图 7-11: 查找异常登录信息

资产选择:	所有分组	▼ 服务器IP或	洺称		服务器标签	搜索	C
告警类型:	异地登录	爆破登录	非法IP登录	非法帐号登录	非法时间登录		
状态: 🗦	未处理 已	处理					

4. 处理异常登录信息。

选择异常登录信息,判断是否存在误报。

- 如果是误报,直接单击标记为已处理。
- 如果是非法入侵,对服务器进行安全加固(例如设置复杂密码,修复服务器漏洞,修复基线 检查的风险点,设置黑/白名单等),完成后单击标记为已处理。

7.4.1.2 设置登录安全策略

设置登录安全策略,包括常用登录地、合法登录IP、合法登录时间和合法账号。

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 入侵检测 > 异常登录。
- 3. 在**异常登录**页面右上角,单击**登录安全设置**。
- 4. 设置常用登录地。
 - a) 单击**添加**。
 - b) 在下拉菜单中选择常用登录地。
 - c) 设置常用登录地对哪些服务器生效。
 - 全部资源中可以选择具体服务器。
 - 分组资产中可以根据分组信息选择服务器。
 - d) 单击确定,完成新增规则操作。
 - e) 选择具体规则, 单击编辑修改规则。
 - f) 选择具体规则, 单击**删除**删除规则。
- 5. 设置合法登录IP。
- 6. 设置合法登录时间。
- 7. 设置合法账号。

7.4.2 网站后门

安骑士采用本地查杀 + 云查杀体系,拥有定时查杀和实时防护扫描策略,支持检测常见的PHP、JSP等后门文件类型,并提供一键隔离功能。

安骑士通过检测您服务器上的Web目录中的文件,判断是否为Webshell木马文件。如果发现您的服务器存在网站后门文件,将会触发告警信息。

安骑士网站后门检测采用动态检测及静态检测两种方式:

- 动态检测:一旦 Web 目录中的文件发生变动,安骑士将会针对变动的内容进行动态检测。
- 静态检测:每天凌晨,安骑士将会扫描整个 Web 目录进行静态检测。

📋 说明:

默认情况下,安骑士防护的所有服务器均开启静态检测。如果需要设置特定服务器开启静态检测,可以在**设置 > 安全设置**中的**木马查杀**区域,单击**周期检查Web目录**右侧的**管理**设置需要进行静态检测的服务器。

7.4.2.1 管理网站后门

查看和隔离网站后门文件。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 入侵检测 > 网站后门。
- 3. 选择资产,查看已发现的网站后门文件记录,如图 7-12: 选择资产所示。

图 7-12: 选择资产

资产选择:	所有分组	•	服务器IP或名称	服务器标签	搜索
状态: 🗦	未处理	已处理			

- 4. 处理网站后门文件。
 - 隔离:对发现的木马文件进行隔离操作,支持批量处理。
 - 恢复:如果错误隔离了某些文件,您可以单击恢复,将此文件恢复。
 - 忽略: 忽略该木马文件后, 安骑士将不再对此文件提示风险告警。

说明:

安骑士不会将您服务器上的木马文件直接删除,只会将该文件转移到隔离区,在您确认该文件为信任文件后可通过恢复功能将该文件恢复,并且安骑士将不再对此文件进行告警。

7.4.3 主机异常

查看在服务器上检测到的异常进程行为和恶意进程等。

7.4.3.1 管理主机异常

查看服务器上的主机异常告警,并修复相应问题。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 入侵检测 > 主机异常。
- 3. 选择资产, 查看已发现的主机异常事件。
- 4. 根据主机异常事件影响情况,选择相应的处理方式,如表 7-6:处理主机异常事件所示。

表 7-6: 处理主机异常事件

操作	说明
一键修复	直接修复漏洞。
忽略本次	如果该事件不影响服务器安全,可以选择忽略本次告警。
确认事件	确认该事件。
标记为误报	如果本次告警为误报,可以标记为误报。
查看	查看本次告警详细信息。

7.5 主机指纹

主机指纹功能定期收集并记录服务器上的运行进程、系统账号、开放端口和软件版本,帮助您全面 了解资产的运行状态和进行回溯分析。

7.5.1 管理监听端口

定期收集服务器的对外端口监听信息,用于清点端口。

背景信息

监听端口应用场景包括:

- 清点一个端口被哪些服务器监听。
- 清点一台服务器开通了哪些端口。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 主机指纹,选择监听端口页签。
- 查看所有已开放端口、端口对应的网络协议、和开放这些端口的主机数。
 您可以通过端口号或进程名搜索,快速查找端口。
- 4. 单击端口号,查看对应的资产、协议等详细信息。

7.5.2 管理运行进程

定期收集服务器的进程信息,用于清点进程。

背景信息

运行进程应用场景包括:

- 清点一个进程被哪些服务器运行。
- 清点一台服务器运行了哪些进程。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 主机指纹,选择运行进程页签。
- 查看所有运行中进程和运行这些进程的主机数。
 您可以使用进程名或运行用户进行搜索。
- 4. 单击进程名,查看进程对应资产、路径、启动参数等详细信息。

7.5.3 管理账号信息

定期收集服务器的账号信息,用于清点账号。

背景信息

账号信息应用场景包括:

- 清点一个账号被哪些服务器创建。
- 清点一台服务器创建了哪些账号。

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 主机指纹,选择账号信息页签。
- 3. 查看所有已登录的系统账号和使用这些账号的主机数。

您可以使用账号名进行搜索。

4. 单击账号名,查看对应资产、ROOT权限、用户组等详细信息。

7.5.4 管理软件版本

定期收集服务器的软件版本信息,用于清点软件资产。

背景信息

软件版本应用场景包括:

- 清点非法软件资产(非法安装)。
- 清点版本过低软件资产。
- 漏洞爆发时快速定位受影响资产范围。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 主机指纹,选择软件版本页签。
- 查看所有使用中的软件和使用这些软件的主机数。
 您可以使用软件名、版本名或软件安装目录进行搜索。
- 4. 单击软件名,查看其对应资产、软件版本等信息。

7.5.5 设置主机指纹刷新频率

通过主机指纹设置功能,选择运行进程、系统账号、开放端口、软件版本数据的收集刷新频率。

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 主机指纹, 单击主机指纹设置。
- 3. 在相应项目的下拉菜单中,选择刷新频率。
- 4. 单击确认,完成配置。

7.6 日志检索

全面支持主机的进程启动、网络连接、系统登录流水等日志查询和导出,便于您进行安全事件分 析、操作日志审计。

7.6.1 日志检索介绍

云主机安全提供主机日志检索功能,将散落在阿里云各系统中的日志集中管理,便于您在出现主机问题时一站式搜索定位问题根源。

支持180天以内的日志存储,并提供30天以内的日志查询。

功能特性

日志检索功能具备以下特性:

- 一站式日志检索平台,集中查询专有云各产品日志,单一接口,便于问题溯源。
- 日志功能的SaaS化,无需进行额外安装部署,即可查询所有云环境中的服务器日志。
- 支持TB级数据检索,以及50个维度的数据逻辑(布尔表达式)组合,可以秒级展示日志全文检 索结果。
- 支持丰富的主机日志源。
- 支持日志投递,允许您将安全日志导入到日志服务做进一步分析。

应用场景

日志检索帮助您实现以下需求:

- 安全事件分析:主机发生安全事件后,通过日志功能进行调查,评估资产受损范围和影响。
- 操作审计:对主机的操作日志进行审计,对高危操作和严重问题进行细粒度排查。

可检索日志类型

表 7-7: 日志源

日志源	说明
登录流水	系统登录成功的日志记录。
暴力破解	系统登录失败的日志记录。
进程快照	某一时刻主机上的进程运行信息。
端口监听快照	某一时刻主机上的监听端口信息。
账号快照	某一时刻主机上的账号登录信息。

日志源	说明
进程启动日志	主机上进程启动的相关信息。
网络连接日志	主机对外主动连接的日志。

7.6.2 查询日志

搜索和查看主机日志。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**云主机安全 > 日志检索**。
- 3. 设置搜索条件。

表 7-8: 搜索条件说明

搜索项	说明
请选择日志源	支持的日志源,具体内容参考表 7-9: 日志源。
请选择字段	各日志源支持的字段,具体内容参考表 7-9:日志源。
关键字	需要搜索的字段具体关键字。
语法逻辑	语法逻辑包括and、or、not,具体说明参考表 7-17: 语法逻辑说明。
+	在一个搜索条件(一个日志源)下增加多个逻辑判断。
增加一组	增加多个搜索条件(不同的日志源)。

- 4. 单击搜索,查看搜索结果。
 - 重置:如果不需要原来设置的搜索条件,单击重置,搜索条件回到初始状态。
 - 保存搜索逻辑:如果以后需要重用这个搜索条件,单击保存搜索逻辑进行保存。
 - **已保存的搜索**:如果需要执行以前保存的搜索条件,单击**已保存的搜索**,选择已有的搜索条件执行。

7.6.3 各日志源字段说明

本文介绍了日志检索功能可以采集并供检索的原始日志类型和字段说明。

日志检索功能支持您查询下表列述的日志源。您可以单击一个日志源查看其支持的字段信息。

表 7-9: 日志源

日志源	说明
登录流水	系统登录成功的日志记录。
暴力破解	系统登录失败的日志记录。
进程快照	某一时刻主机上的进程运行信息。
端口监听快照	某一时刻主机上的监听端口信息。
账号快照	某一时刻主机上的账号登录信息。
进程启动日志	主机上进程启动的相关信息。
网络连接日志	主机对外主动连接的日志。

登录流水

登录流水查询支持以下字段:

表 7-10: 登录流水支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	登录来源IP
warn_port	string	登录端口
warn_user	string	登录用户名
warn_type	string	登录类型
warn_count	string	登录次数
time	datetime	登录时间

暴力破解

暴力破解查询支持以下字段:

表 7-11: 暴力破解支持字段

字段	数据类型	说明
uuid	string	客户端编号

字段	数据类型	说明	
IP	string	IP地址	
warn_ip	string	攻击来源IP	
warn_port	string	破解端口	
warn_user	string	破解用户名	
warn_type	string	类型	
warn_count	string	破解次数	
time	datetime	破解时间	

进程启动日志

进程启动日志查询支持以下字段:

表 7-12: 进程启动日志支持字段

字段	数据类型	说明	
uuid	string	客户端编号	
IP	string	IP地址	
pid	string	进程ID	
groupname	string	用户组	
ppid	string	父进程ID	
uid	string	用户ID	
username	string	用户名	
filename	string	文件名	
pfilename	string	父进程文件名	
cmdline	string	命令行	
filepath	string	进程路径	
pfilepath	string	父进程路径	
time	datetime	启动时间	

端口监听快照

端口监听快照查询支持以下字段:

表 7-13: 端口监听快照支持字段

字段	数据类型	说明	
uuid	string	客户端编号	
IP	string	IP地址	
src_port	string	监听端口	
src_ip	string	监听IP	
proc_path	string	进程路径	
PID	string	进程ID	
proc_name	string	进程名	
proto	ito string 协议		
time	datetime	数据获取时间	

账号快照

账号快照查询支持以下字段:

表 7-14: 账号快照支持字段

字段	数据类型	说明	
uuid	string	客户端编号	
IP	string	IP地址	
perm	string	是否拥有root权限	
home_dir	string	home目录	
warn_time	string	密码到期提醒时间	
groups	string	用户属于的组	
login_ip	string	最后一次登录的IP地址	
last_chg	string	密码最后修改时间	
shell	string	Linux的shell命令	
domain	string	Windows域	
tty	string	登录的终端	
account_expire string 账号		账号超期时间	

字段	数据类型	说明
passwd_expire	string	密码超期时间
last_logon	string	最后登录时间
user	string	用户
status	string	用户状态: • 0表示禁用 • 1表示正常
time	datetime	数据获取时间

进程快照

进程快照查询支持以下字段:

表 7-15: 进程快照支持字段

字段	数据类型	说明		
uuid	string	客户端编号		
IP	string	IP地址		
path	string	进程路径		
start_time	string	进程启动时间		
uid	string	用户ID		
cmdline	string	命令行		
pname	string	父进程名		
name	string 进程名			
pid	string	进程ID		
user	string	用户名		
md5	string	进程文件MD5值,超过1MB不 计算		
time	datetime	数据获取时间		

网络连接日志

网络连接日志查询支持以下字段:

字段	数据类型	说明	
uuid	string	客户端编号	
IP	string	IP地址	
src_ip	string	源IP	
src_port	string	源端口	
proc_path	string	进程路径	
dst_port	string	目标端口	
proc_name	string	进程名	
dst_ip	string	目标IP	
status	string	状态	
proto	string	协议	
time	datetime	连接时间	

表 7-16: 网络连接日志支持字段

7.6.4 语法逻辑说明

日志检索支持多条件逻辑检索,您可以在一个搜索条件(一个日志源)下增加多个判断逻辑,也可以对多个搜索条件(不同的日志源)进行逻辑组合。本文介绍了日志检索支持的语法逻辑,也列举了部分用例,帮助您理解和使用。

日志检索支持下表中列举的语法逻辑。

表 7-17: 语法逻辑说明

逻辑名称	描述
and	双目运算符。 形式为query1 and query2,搜索结果展示query1和query2查询结 果的交集。
	道 说明 : 如果多个单词间没有语法关键词,默认是and的关系。
or	双目运算符。 形式为query1 or query2,搜索结果展示query1和query2查询结 果的并集。

逻辑名称	描述
not	双目运算符。 形式为query1 not query2,搜索结果展示符合query1并且不符合 query2的结果,相当于query1 - query2。
	说明 : 如果只有not query1,那么表示从全部日志中选取不包含query1的 结果。

7.7 设置

7.7.1 管理安全配置

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 设置。
- 3. 配置对服务器进行周期性木马查杀。
 - a) 单击**管理**。
 - b) 选择哪些服务器需要进行周期性的木马查杀。
 - c) 单击确认,完成配置。
- 4. 配置安骑士Agent资源占用模式。
 - 业务优先模式: CPU占用峰值小于10%, 内存占用峰值小于50 MB。
 - 防护优先模式: CPU占用峰值小于20%, 内存占用峰值小于80 MB。
 - a) 单击**管理**。
 - b) 设置服务器的安骑士Agent工作模式。
 - c) 单击确认,完成配置。

7.7.2 安装安骑士Agent插件

在Windows服务器或Linux服务器上手动安装安骑士Agent插件。

前提条件

如果您已在服务器上安装了安全软件(如安全狗、云锁等),可能会导致安骑士Agent插件无法正常安装,建议您暂时关闭或卸载该安全软件,然后再安装安骑士Agent插件。

背景信息

安骑士Agent插件已集成于公共镜像中。如果您在创建 ECS 实例时选择公共镜像,安骑士Agent插 件将自动集成到ECS实例中。

非阿里云服务器必须通过安装程序(Windows)或脚本命令(Linux)方式安装安骑士Agent 插件。 如果您的非阿里云服务器通过以下方式安装安骑士Agent 插件,需要删除安骑士Agent插件目录 后,按照上述手动安装步骤重新安装安骑士Agent 插件。

- 通过已安装安骑士Agent插件的镜像批量安装服务器。
- 从已安装安骑士Agent插件的服务器上直接复制安骑士Agent插件文件。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 设置 > 安装 / 卸载。

进入安骑士Agent插件安装页面,如图 7-13: Agent安装所示。

图 7-13: Agent安装

如何为金融云平台、VPC环境用户安装插件?	
Windows 系统 Windows 2012 8 Windows 2008 Windows 2003	Linux系统 CentOS: Versions 5,6 and 7 (32/64 bit) Ubuntu: 9.10 - 14.4 (32/64 bit) Debian: Versions 6,7 (32/64 bit) RHEL: Versions 5,6 and 7 (32/64 bit) Gentoc: (32/64 bit) OpenSUSE: (32/64 bit) Aliyun Linux
下载并以管理员权限在您的云服务器上安装 了解更多	1 在您的服务器中以管理员权限执行以下命令进行安装
<u>「</u> 」「「」」「」」「」」「」」「」」「」」「」」「」」「」」」	⑧ 阿里云服务器 ◎ 非阿里云服务器
2 非阿里云服务器需输入以下安装验证key	wget "https://update3.aegis.aliyun.com/download/AliAq sinstall_32.sh" && chmod +x AliAqsinstall_32.sh && ./Ali AqsInstall_32.sh 7a5GDk
	wget "https://update3.aegis.aliyun.com/download/AliAq sinstall_64.sh" && chmod +x AliAqsInstall_64.sh && ./Ali Aqsinstall_64.sh 7a5GDk
安发成初后,寺侍人约5-10万钟时在页广中宣君到,处即宣君。	

3. 根据您的服务器操作系统,获取并安装安骑士Agent插件。

• Windows系统

- 1. 在左侧区域,单击点击下载,下载安装文件到本地计算机。
- 2. 将安装文件上传至您的Windows服务器。例如,您可以通过FTP工具,将安装文件上传到服务器。

3. 在Windows服务器上,以管理员权限运行安装文件,完成安装。

在非阿里云服务器上安装Agent插件的过程中,您会收到提示,要求您输入安装验 证Key。您可在安骑士Agent插件安装页面找到您的安装验证Key。

• Linux系统

- 1. 在右侧区域,根据您的实际情况,选择阿里云服务器或非阿里云服务器。
- 2. 根据您的操作系统类型,选择32位或64位的安装命令,单击复制。
- 3. 以管理员身份登录您的Linux服务器。
- 4. 在Linux服务器上执行安装命令,下载和安装安骑士Agent插件。
- 4. 查看服务器在线情况。

安骑士Agent 插件安装完成约五分钟后,可以在云盾服务器安全(安骑士)管理控制台中查看您 服务器的在线情况:

- 阿里云服务器将会从离线变成在线。
- 非阿里云服务器将会被添加至您的服务器列表中。

7.7.3 卸载安骑士Agent插件

如果云主机不再使用安骑士服务的所有功能,可以选择以下方式进行卸载安骑士Agent插件。

背景信息

通过控制台卸载指定主机安骑士Agent,请务必确保当前机器安骑士Agent处于在线状态,否则无法 接收到卸载指令。

如果卸载后重新安装安骑士Agent,请手工进行安装,忽略期间的报错,重复操作3次以上(安骑士 Agent卸载会有一段保护期24小时或重复执行3次以上安装命令)。

- 1. 登录云盾安全中心。
- 2. 定位到云主机安全 > 设置 > 安装 / 卸载。
- 3. 单击右上角的卸载安骑士。
- 4. 在卸载提示对话框中,选择要卸载安骑士Agent插件的服务器。
- 5. 单击确认卸载,系统将自动卸载安骑士Agent插件。

8 物理机防护

8.1 查看并处理文件篡改事件记录

监控主机系统特定目录中文件的完整性,及时发现篡改行为并进行告警。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到物理机安全 > 物理机防护页面,选择文件篡改。
- 3. 查看文件篡改事件记录,如图 8-1:文件篡改事件记录所示。

图 8-1: 文件篡改事件记录

主机入	侵检测									
分类:	分类: 文件書記 异常均衡注意 可能测口监听									
状态: 🖆	全部 • 服务	器IP,支持模糊团	節 文件目录 , 支持	模糊查询 变动	时间: 起始时间	至终止时间	接線			
	服务器IP	区域	文件目录	变动类型	变动时间	原始文件创建时间	变动详情	状态	操作	
	0.05.630	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:06	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理	
	308409	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:13	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理	
	203.638	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:07	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理	
	10.00	缺省机房	/etc/init.d/docker	文件新建	2017-07-01 15:10:39	2017-07-26 10:52:06	新建文件md5:997dbb021a2d1ca7455c73e2e5a84aea	未处理	标记为已处理	
	303.648	缺省机房	/etc/init.d/mysql	文件修改	2017-07-26 01:26:10	2017-06-23 21:56:03	源文件md5:176bd7a935c0ebb8b308f65a4db3d441 修改后文件md5:176bd7a935c0ebb8b308f65a4db3d441	已标记处理	-	

- 4. 进一步排查该文件篡改事件。
 - 如确认该事件为异常事件,请立即对该服务器采取安全加固措施,并建议进一步检查、分析 被入侵的原因。
 - 如确认该事件为正常事件或已处理完该入侵事件,单击标记为已处理,在弹出的对话框中单击确定,将该事件标记为已处理。

8.2 查看并处理异常进程记录

及时发现异常进程启动,并进行告警。

- 1. 登录云盾安全中心。
- 2. 定位到物理机安全 > 物理机防护页面,选择异常进程。
- 3. 查看异常进程记录,如图 8-2:异常进程记录所示。

图 8-2: 异常进程记录

主机入	主机入侵检测										
分类: 3	分泌 文件截波 异物网络连接 可照顾口篮听										
状态: 🖻	と部 ▼ 服务器IP,支持	朦朧直询 进程路径,支持模	糊查询 启动时间: 起始	时间至	终止时间	搜索					
	服务器IP 区域	进程路径	进程类型	启动时间	文件大小	文件hash值	文件创建时间	状态	操作		
	2020.01	/etc/rc.d/init.d/selinux	gate_backdoor_file	2017-07-17 17:30:17	8464	4a8e5735fefe17ec4410e5e4889dca3a	2017-06-29 16:15:44	未处理	标记为已处理		
	1010.00	/usr/bin/pamdicks	rootkitminer_file	2017-07-15 17:54:37	11128	f679115e75735c2de5937448b30242b8	2017-07-11 21:19:03	未处理	标记为已处理		
	3038.63	/boot/vfpjyckqma	gate_xordoor_file	2017-07-15 19:50:06	8464	e0bc372135f57507a7689bd3069c705a	2017-06-29 16:15:56	未处理	标记为已处理		
	0.05.65	/etc/rc.d/init.d/selinux	gate_backdoor_file	2017-07-17 17:30:17	8464	4a8e5735fefe17ec4410e5e4889dca3a	2017-06-29 16:15:44	未处理	标记为已处理		
	30840	/usr/bin/pamdicks	rootkitminer_file	2017-07-15 17:54:37	11128	f679115e75735c2de5937448b30242b8	2017-07-11 21:19:03	未处理	标记为已处理		
	203.43	/boot/vfpjyckqma	gate_xordoor_file	2017-07-15 19:50:06	8464	e0bc372135f57507a7689bd3069c705a	2017-06-29 16:15:56	未处理	标记为已处理		

- 4. 进一步排查该异常进程。
 - 如确认该进程为异常进程,请立即对该服务器采取安全加固措施,并进一步检查、分析被入 侵的原因。
 - 如确认该进程为正常进程或已处理完该异常进程事件,单击标记为已处理,在弹出的对话框
 中单击确定,将该事件标记为已处理。

8.3 查看并处理异常网络连接记录

及时发现主动外连公网的网络连接,并进行告警。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到物理机安全 > 物理机防护页面,选择异常网络连接。
- 3. 查看异常网络连接记录,如图 8-3:异常网络连接所示。
 - 图 8-3: 异常网络连接

主机入	主机入侵检测							
分类: : :	文件篡改 异常进程 异常网络连接	可疑論口监听						
状态: 👔	全部 v 服务器IP,支持模糊图	管询 进程路径,支持	持模糊查询 连接时间: 1	國始时间	至终止时间 搜索			
	服务器IP 区域	事件类型	连接时间	对应进程	进程路径	连接详情	状态	操作
	10.00.04.0	Connect Internet	2017-06-16 17:42:25	7116	/apsara/cloud/app/tianji/TianjiClient#/proxyssl/237727/proxyssl	访问源:10.35.6.90:44231 访问目标:127.0.0.1:12344	未处理	标记为已处理
	10.00.04.0	Connect Internet	2017-06-16 17:42:31	7223	/apsara/cloud/app/tianji/TianjiClient#/p2p_worker/237727/p2p_worke r	访问源:10.35.6.90:29686 访问目标:127.0.0.1:7070	未处理	标记为已处理
	HALPO -	Connect Internet	2017-06-16 20:13:26	3727	/apsara/cloud/app/tianji/TianjiClient#/proxyssl/237727/proxyssl	访问源:10.35.6.74:3078 访问目标:127.0.0.1:12344	未处理	标记为已处理
	HALFS-	Connect Internet	2017-06-16 20:13:32	3784	/apsara/cloud/app/tianji/TianjiClient#/p2p_worker/237727/p2p_worke r	访问源:10.35.6.74:12384 访问目标:127.0.0.1:7070	未处理	标记为已处理

4. 进一步排查该异常网络连接。

- 如确认该进程为异常连接,请立即对该服务器采取安全加固措施,并进一步检查、分析被入 侵的原因。
- 如确认该进程为正常连接或已处理完该异常网络连接事件,单击标记为已处理,在弹出的对 话框中单击确定,将该事件标记为已处理。

8.4 查看并处理异常端口监听记录

及时发现异常的端口监听,并进行告警。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到物理机安全 > 物理机防护页面,选择可疑端口监听。
- 3. 查看异常端口监听记录,如图 8-4:异常端口监听记录所示。

图 8-4: 异常端口监听记录

主机	主机入侵检测								
分类:	398. 文件描述 异型进程 异烟烟虫油 a 可以自己的听								
状态:	全部 🔻 服务器	iP,支持機糊查询	端口	进程路径,支持模糊团	询 变动时间: 起始时间	至终止时间	搜索		
	服钙器IP	区域	监听端口	开始监听时间	对应进程	进程路径	说明	状态	操作
	30.06447	缺省机房	37308	2017-06-29 16:28:01	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异策端口	未处理	标记为已处理
	3038.675	缺省机房	51015	2017-06-29 16:28:03	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	10.00.00	缺省机房	53638	2017-06-29 16:28:04	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	3028.643	缺省机房	45564	2017-06-29 16:28:01	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	10.00.001	缺省机房	53693	2017-06-29 16:28:01	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理
	3006443	缺省机房	47402	2017-06-29 16:28:05	/usr/ali/jdk1.6.0_16/bin/java	/usr/ali/jdk1.6.0_16/bin/java	异常端口	未处理	标记为已处理

- 4. 进一步排查该异常端口监听。
 - 如确认该进程为异常监听事件,请立即对该服务器采取安全加固措施,并进一步检查、分析 被入侵的原因。
 - 如确认该进程为正常端口监听或已处理完该异常监听事件,单击标记为已处理,在弹出的对 话框中单击确定,将该事件标记为已处理。

9 资产总览

云盾安全中心通过图表方式展现当前用户资产的总数(分为主机资产、NAT资产)、增减频率、以及区域分布等统计信息,并按分组、类型供安全管理员查询资产的相关信息,帮助安全管理员从整体了解资产情况,以便更好地管理资产。

安全管理员可以在**资产管理 > 资产总览**页面,直观了解到资产概览信息,包括资产总数、本月新 增资产数、分组数目、区域数目、资产上报时间分布图、资产所属分组分布图、资产所属区域分布 图,帮助用户更好地管理资产,如图 9-1:资产总览页面所示。



图 9-1: 资产总览页面

表 9-1: 资产总览页面参数说明表

参数	说明
资产总数	安骑士客户端上报的资产总数,包含主机资产和NAT资产。
本月新增资产数	本月新增的资产总数,包含主机资产和NAT资产。
资产时间分布图	七天内资产数量的变化情况,分主机资产、NAT资产进行统计。
分组数目	当前已有的分组数目。
资产分组分布图	资产分组比例图是按每个分组内的资产数占总资产数目的比例计算的。
区域数目	当前配置的区域数目。
资产区域分布图	资产区域分布图是按每个区域内的资产数占总资产数目的比例计算的。

9.1 分组管理

分组管理主要用于对资产分组的增加、删除、重新排序。将资产分组,用于区分不同资产的特定作用,便于查询资产信息并对资产信息进行修改。

说明:

- 资产分组最多只支持10个分组。
- 默认分组不可被删除且不可更改名称。
- 资产分组中存在资产时不可被删除。

9.1.1 添加分组

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到资产管理 > 资产总览页面,单击分组管理。

图 9-2: 分组管理

分组:	全部(6台)					
				i) <u>分组管理</u>		
主机资	■ NAT资产					

3. 在弹出业务分组对话框,单击添加分组,如图 9-3:业务分组对话框所示。

图 9-3: 业务分组对话框

业务分组			\times
()(01.		TH	
万祖1:	安主同识-初期	P49	
分组2:	测试分组1	上移下移 删除	
分组3:	测试分组2	上移 下移 删除	
分组4:	交换1	上移下移删除	
分组5:	默认分组	上移 下移	
分组6:	云盾集群1	上移 下移	
分组7:	新増1	上移下移 删除	
分组8:	交换212312312	上移 下移	
分组9:	test123	上移	
	添加分组 最多只能添加10个分组!		
		确认 取消	

- 4. 填写分组名称。
- 5. 单击确认,添加资产分组。

9.1.2 删除分组

- 1. 登录云盾安全中心。
- 2. 定位到资产管理 > 资产总览页面,单击分组管理。
- 3. 在业务分组对话框内,单击对应分组条目后的删除,如图 9-4: 删除业务分组所示。

图 9-4: 删除业务分组

分组3:	测试服务器	上移	下移	删除

4. 单击确认,删除该资产分组。

9.1.3 调整分组排序

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到资产管理 > 资产总览页面,单击分组管理。
- 3. 通过单击业务分组对话框内各个条目后的上移、下移进行排序调整。
- 4. 单击确认,完成资产分组的排序调整。

9.2 资产信息

资产分为主机资产和 NAT 资产,两种资产的信息和管理方式略有差异,可以通过切换查看不同类型的资产信息。

表 9-2: 资产类型表

资产类型	说明
主机资产	安骑士客户端防护的服务器资产。
NAT资产	内网地址经过NAT转换,暴露给外网的IP资产。

9.2.1 管理主机资产

主机资产主要是指服务器资产,安装安骑士客户端并连接到服务器后,将会上报为资产。

背景信息

通过查询主机资产,安全管理员可以掌握各资产的大致情况,例如操作系统、开放端口、已安装的 常用软件,也可以对资产的区域和分组进行调整。

- 1. 登录云盾安全中心。
- 2. 定位到资产管理 > 资产总览页面,选择主机资产。

3. 设置查询条件,单击查询,查看主机资产信息,如图 9-5:主机资产页面所示。

▋ 说明:

主机资产的查询支持根据操作系统、区域、分组进行筛选,并支持通过主机IP及主机名进行模糊查询。默认情况下,主机资产页面展示全部区域,并按照IP排序。

图 9-5: 主机资产页面

主机资产	NAT资/ ^m							
操作系统/版本:	金郎 1 输入P/主机名	18 B						9324 939#
主机IP/主机名	i de la companya de l	uuld	所属用户	所属业务	所属区域	操作系统版本	主机端口	18:19
192.168.250. IZys805xw0p	87 cswq03p3y86Z	8bcc802e-108d-48d1-b973-6744863cd153	Frank'sDept	默认分组	cn-hangzhou-env6-d01	Linux/CentOS release 5.11 (Final)/2.6.18-418.el5	評問	修改 删除 展开应用信息。
192.168.242. IZudiyzthgfn4	112 Z	7fa23022-c537-48a7-82b1-78df1e3154d1	研发	默认分组	cn-hangzhou-env6-d01	Microsoft Windows Server 2008 R2 Enterprise Edition Service Pac k 1 (build 7601), 64-bit	37M	律改 删除 展开应用信息+
192.168.242.1 IZys605vkyv9	111 Jak5dmn089Z	bb79d874-0c22-4222-b53c-5a4b46a4ab80	研究	默认分组	cn-hangzhou-env6-d01	Linux/CentOS release 6.8 (Final)/2.6.32-642.13.1.el6x86_64	99	停改 删除 展开应用信息 =
192.168.242. 云唐堂是机测	110 30.41.84-00 部	ca858232-0c7c-4e8b-a18a-32b1a582aceb	研发	默认分组	cn-hangzhou-env6-d01		20 M	体改 删除 展开应用信息。

- 4. 选择主机,查看详细信息。
 - 单击详情,可以查看主机端口开放情况。
 - 单击展开应用信息,可以查看主机已有的可监测应用信息。
- 5. 维护主机资产信息。
 - 单击修改,在修改资产信息对话框修改所属资产分组及所属区域,单击确定,如图 9-6:修改 资产信息对话框所示。

图 9-6: 修改资产信息对话框

修改资产信息		\times
主机IP		
主机名		
所属业务	默认分组 ▼	
操作系统/版本	Linux/CentOS release 5.11 (Final)/2.6.18-418.e	
所属区域	· · · · · · · · · · · · · · · · · · ·	
	确定取	肖

• 单击删除,在资产信息删除对话框中单击确定进行删除。

📃 说明:

如果在云服务器中卸载了安骑士客户端,或者在专有云平台中删除了一台ECS云服务器,这些主机对应的资产需要手动删除。

9.2.2 管理NAT资产

NAT资产,也可以理解为IP资产,是指内网地址经过NAT转换来访问互联网的IP资产,即暴露给外网的IP地址资产。该IP可能会被很多主机使用,不同端口可以指向不同主机。当IP被设置为NAT资产后,态势感知模块会对其进行分析,从而发现一些攻击事件。

背景信息

通过查询NAT资产,安全管理员可以了解当前云盾防护的NAT资产的基本信息,也可以对资产进行 分组和区域的修改,NAT资产支持单个资产添加以及按网段批量添加。

操作步骤

1. 登录云盾安全中心。

2. 定位到资产管理 > 资产总览页面,选择NAT资产。

3. 设置查询条件,单击查询,查看NAT资产信息,如图 9-7: NAT资产页面所示。

送明:

NAT资产的查询支持通过区域、分组进行筛选,支持根据IP进行模糊查询。默认情况下,NAT资产页面展示全部区域,并按照IP排序。

图 9-7: NAT资产页面

IT/8/* MT8/*				
MEER BE . BANT P BR				1850 6 353/4
NAT IP	所服业内	MEEN	MD CH	80
10.000.000.000	BH3.940	大州机器	178	1721 Bile
11000.000.000	IN3.948	大兴机构	28	1000 (1000
1.02.03.03	Invest.	大大的唐	28	1721 Bio
11-10-10-10-10	INV.948	7.HTM	28	972 Bie
1.02.03.03	100.948	大兴的唐	28	900 i 800
11-12-12-12	INV.942		28	60X 804
11.02.03.03	INV.SHE	大大的時	28	1000 (1000
11-12-12-12	tel:	大开的唐	28	1722 Bile
1.8.81	INV.948	大片的 网	28	900 (Bib
				月49日,4月2日:20日 × × 1 > >

4. 添加新的NAT资产。

添加的资产IP不能与当前已有IP冲突。NAT IP字段必须为合法IP或者为合法网段。

- a)在NAT资产页面,单击列表右上方的添加。
- b) 在**添加资产信息**对话框中,输入IP地址或者IP表达式,选择所属业务和所属区域。
- c) 单击**确定**。
- 5. 维护NAT资产信息。
 - 单击**详情**,可以查看该NAT资产的端口开放情况。
 - 单击修改,在修改资产信息对话框中,修改该资产所属业务分组和所属区域,单击确定,如图 9-8:修改资产信息对话框所示。

图 9-8: 修改资产信息对话框

修改资产信息		×
NatIP		
所属业务	默认分组	v
所属区域		•
		确定取消

• 单击删除,在资产信息删除对话框中单击确定,可删除该NAT资产。

9.2.3 批量修改资产所属分组或区域

背景信息

资产管理功能支持通过两种方式来修改资产的所属分组和所属区域:单个修改和批量修改。

- 单个修改适用于需要修改信息的资产数量只有一台;或者,需要修改的资产既不在同一网段,主 机名也没有任何规律。单个资产的修改方法,参见管理主机资产和管理*NAT*资产。
- 批量修改适用于对多台资产进行修改并且这些资产属于同一个网段或拥有相似的主机名。



主机IP、主机名和操作系统/版本是资产的固有信息不能修改。

- 1. 登录云盾安全中心。
- 2. 定位到资产管理 > 资产总览页面。
- 3. 修改资产所属分组或所属区域。
 - 单击修改分组,批量修改资产分组。
 - 单击修改区域,批量修改资产区域。
- 在修改分组或修改区域对话框中,根据实际情况设置批量修改范围,选择这些资产需要分配到的 资产分组或区域,单击确定。
 - 选择网段类型,输入所需批量修改的主机资产或NAT资产的所属网段。
 - 选择**主机名**类型,输入所需批量修改的主机资产主机名所共有的部分。



- 使用网段类型进行批量修改,符合所设置的网段范围的主机资产和NAT资产都会被修改。
- 使用主机名类型进行批量修改,只有符合所设置的主机名范围的主机资产被修改。

10 安全审计

安全审计是指由专业审计人员根据有关法律法规、财产所有者的委托和管理当局的授权,对计算机 网络环境下的有关活动或行为进行系统的、独立的检查验证,并作出相应评价。在管理员需要对系 统过往的操作做回溯时,可以进行安全审计。

安全审计是一项长期的安全管理活动,贯穿云服务使用的生命周期。云盾的安全审计能够收集系统 安全相关的数据,分析系统运行情况中的薄弱环节,上报审计事件,并将审计事件分为高、中、低 三种风险等级,安全管理员关注和分析审计事件,从而持续改进系统,保证云服务的安全可靠。

10.1 查看审计一览

审计一览页面提供原始日志趋势、审计事件趋势、审计风险分布、危险事件分布四种报表。报表以 趋势图或饼图的方式直观地呈现给安全管理员,便于分析云服务面临的风险趋势。

背景信息

- **原始日志趋势**的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的日志个数。通过云平台日志趋势,安全管理员可以了解系统产生的日志数量是否正常。
- 审计事件趋势的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的审计事件 个数。通过审计事件趋势,安全管理员可以了解系统产生的审计事件数量是否正常。
- **审计风险分布**的数据是一周内高风险、中风险、低风险事件的个数。通过审计风险分布,安全管 理员可以了解系统产生的审计事件级别是否正常。
- 危险事件分布的数据是一周内不同事件类型占总事件的比例。通过危险事件分布,安全管理员可以了解什么类型的审计事件占比较多,识别高风险问题,做好预防措施。

同时,在**审计一览**页面,安全管理员还可以了解指定时间范围内所有审计类型的日志量信息及存储 用量情况。

- 1. 登录云盾安全中心。
- 2. 定位到安全审计 > 审计一览,进入审计一览页面,如图 10-1: 审计一览页面所示。

图 10-1: 审计一览页面

申计一范 単止25時: 回回25月 8月 申计5月前至第: 2015-1-3 - 2015-1-9	
审计规型: N AI N 数据库 N 主机 N 网络设备 N 用个操作 N 添加操作	
原始日本尴尬	审计事件趋势
1 5004	200 - 前規電 - 三規 - 三 - 三 - 三 - 三 - 三 - 三 - 三 - 三
	Britisk

3. 选择截止时间,单击查看,即可查看截止至该时间一周内的审计一览信息。

送 说明: 在**审计时间范围**可以查看当前显示的审计日志信息的具体时间范围。

4. 勾选审计类型,可以选择是否显示该类型的审计日志信息。

10.2 查询审计事件

审计查询页面可查看日志创建时间、审计类型、审计对象、操作类型、风险级别、日志内容等审计 事件的详细信息。

背景信息

审计事件生成的过程:将安全审计模块收集到的日志匹配审计规则,如果日志内容能匹配任意一条 审计规则的正则表达式,就会上报审计事件。关于审计策略规则,参见新增审计策略。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到安全审计 > 审计查询,进入审计查询页面。
- 3. 设置查询条件和查询时间,单击查询,查看该时间段内发现的审计事件。

基础查询条件包括审计类型、审计对象、操作类型、操作风险级别等。

单击高级查询,可设置更详细的过滤条件,包括发起者、目标、命令、结果、原因等。

4. 单击导出,创建导出任务。

导出的文件,如果需要下载到本地分析,可以参考管理导出任务。

10.3 查看原始日志

在**原始日志**页面中,可查看审计对象在运行时产生的原始日志。原始日志作为必要的调试信息,安 全管理员可以根据这些日志信息定位系统出现的故障。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到安全审计 > 原始日志,进入原始日志页面,如图 10-2: 原始日志页面所示。

图 10-2: 原始日志页面



3. 选择审计类型和审计对象,设置查询时间,单击查询,查看该时间段内指定审计对象的原始日志 信息,如图 10-3: 原始日志信息所示。

图 10-3: 原始日志信息

时间	來遊	日志内容
2018-01-09 10:43:00	10.36.9.62	db: indb3 ooi960 ooi900 hat::::::::::::::::::::::::::::::::::::
2018-01-09 10:43:00	10.36.9.62	db: insdb2 ordpit_Unit: 151445780724499 mot: 0 hant: 759718334 return_rows: 0 fc: 10 scil.com accessf kebrory: 117 febrory: 107 fc: 0 scil.com accessf kebrory: 117 fc: 0 fc: 0 scil.com accessf kebrory: 117 fc: 0 fc: 0 fc: 0 scil.com accessf kebrory: 117 fc: 0 fc:

4. 单击导出,创建导出任务。

导出的文件,如果需要下载到本地分析,可以参考管理导出任务。

10.4 策略设置

10.4.1 配置审计策略

10.4.1.1 新增审计策略

当日志记录匹配审计策略中的规则时,就会上报审计事件。

背景信息

审计规则支持匹配正则表达式。正则表达式描述了一种字符串匹配的模式,可以用来检查一个串是 否含有某种子串。例如:

正则表达式	说明
^\d{5,12}\$	表示匹配第5到第12位的连续数字
load_file\(表示匹配 "load_file(" 字符串

安全审计模块根据发生审计事件时日志中输出的字符串,定义了默认的审计策略。安全管理员也可 以根据受到攻击时日志输出的字符串自定义审计策略。

- 1. 登录云盾安全中心。
- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择审计策略页签, 如图 10-4: 审计策略页面所示。

图 10-4: 审计策略页面

审计策略	美型设置 告警谈	置 存档	き理 导出き	2理				
审计类型:	数据库 ▼ 审计对象:	全局		Ŧ	查询			新増
规则ID	策略名称	审计类型	审计对象	时间	关键字段	风险级剧	规则类型	操作
10202	数据库攻击规则	数据库	全局	2017-12-15 13:20:33	sql REGEX "asciil(substr/(sys_context" OR sql REGEX "sleep.(0,1 5)(lengthJascii)" OR sql REGEX "wsc["-0-9a-2]+(master/ubo),Im aster(,1,)?[si)p" OR sql REGEX "load_file()" OR sql REGEX "select (s(0,10){-{(1,15)}s(1,20)})e(0,10)?mm/s(0,10){-{(1,15)}s (1,30)}" OR sql REGEX "(?:ti\r/in)rl/if(l+1)-(1)-[0](5))waltor (?:\r(TS)=??*/T)sltir/in1/fil/ul+1-[1/*V)-dels(?:1)^*(2)- (s]*?*("ls]!tir/in)rl/if(l+1)-(1+"V)+{(1,17)}-dels(?)(?)*(TS s]*?*("ls]!tir/in)rl/if(l+1)-(1+"V)+{(1,17)}-dels(?)(3)* OR s ql REGEX "(tk]!r/in)rl/if(l+1)-(1+"V)+{(1,17)}-dels(?)(3)* OR s ql REGEX "(tk]!r/in)rl/if(l+1)-(1+1)-(1+"V)+{(1,17)}-dels(?)(1+1)-(1+"V)+{(1,17)}-dels(?)(1+1)-(1+1)-(1+"V)+{(1,17)}-dels(?)(1+1)-(1+1)	高危风险事件	默认	禁用

- 4. 单击**新增**。
- 5. 在新增规则对话框中,设置审计规则,如图 10-5:新增规则对话框所示。

图 10-5: 新增规则对话框

新增规则			\times
策略 审计类型: 操作风险	名称 n 数据库 级别: 高危	le01 ▼ 审计对象: 全局 ▼ 操作类型: 数据库攻击 ▼ 风险事件 ▼ 是否告答: 告答 ▼	
过滤条件:			
发起者	等于 🔻	输入发起者关键字 x +	Â
目标	等于 ▼	输入目标关键字 x +	
命令	等于 🔻	输入命令关键字 x +	
结果	等于 ▼	输入结果关键字	
原因	等于 🔻	输入原因关键字	
备注	备注		
			•
		添加取	消

6. 单击**添加**。

添加审计策略后,在指定的审计类型、审计对象、风险级别的审计日志中,如果出现匹配正则表达式的内容,会发送一封告警邮件给已设置的报警接收人。

10.4.1.2 管理审计策略

审计策略是正则表达式规则,当日志记录中的某个字符串匹配审计规则的正则表达式,就会上报审计事件。

操作步骤

1. 登录云盾安全中心。

- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择**审计策略**页签。
- 4. 选择审计类型和审计对象,单击查询,查询审计策略。
- 5. 在查询结果中,单击删除,可删除该审计策略。



系统默认的审计策略无法删除。

6. 在查询结果中,单击启用或禁用,可设置该审计策略是否生效。

说明:

新增的审计策略默认为启用状态。

10.4.2 管理操作类型

新增、查询和删除审计策略的操作类型。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择类型设置页签,如图 10-6:操作类型设置页面所示。

图 10-6: 操作类型设置页面

审计策略 类型设	·查 告答设置 存档管理	导出管理			
审计类型: 数据库	▼ 审计对象 全局		▼ 直询		aita:
名称	审计类型	审计对象	创建时间	说明	损作
数据库攻击	数据库	全局	2017-12-15 13:20:33	数据库攻击	809
				Total: 1 item(s) , Per Page: 20 item(s) « <	1 > >

- 4. 新增操作类型。
 - a) 单击新增。
 - b) 在新增事件类型对话框中,配置事件类型,如图 10-7:新增事件类型所示。

图 10-7: 新增事件类型

新增事件类型				\times
名称	请输入操作类型简称			
审计类型	数据库	•		
审计对象	全局	•		
说明				
			确定	取消

- c) 单击**确定**。
- 5. 查询操作类型。

选择审计类型和审计对象,单击查询,查看当前已设置的操作类型。

6. 删除操作类型。

在查询结果中,单击删除,可删除该操作类型。

_____ 说明∶

系统默认的操作类型无法删除。

10.4.3 设置告警接收人

设置报警接收人的邮箱,在发生审计事件后,会将事件上报到所设置的告警人的邮箱。

- 1. 登录云盾安全中心。
- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择告警设置页签,如图 10-8:告警设置页面所示。

图 10-8: 告警设置页面

审计策略	类型设置	告警设置	存档管理	导出管理							
审计类型:	全部 🔻	审计对象: 全	語		•	输入邮箱	风险等级:	全局风险	▼ 查询		新增
邮箱				审计类型	2	审计对象			姓名	风险等级	操作
	@alibaba-inc.	com		用户操作	ŧ	yundun-advance操作日志			vanghaitao	全局风险	删除

- 4. 新增告警接收人。
 - a) 单击**新增**。
 - b) 在新增报警接收人对话框,配置告警接收人信息,如图 10-9:新增报警接收人对话框所示。

图 10-9: 新增报警接收人对话框

新增报警接收人		×
邮箱	请输入有效邮箱eg:xxx@xxx	
姓名	请输入姓名	
审计类型	全部	•
审计对象	全部	•
风险等级		•
		确定 取消

- c) 单击**确定**。
- 5. 查询告警接收人。

选择审计类型、审计对象、风险等级,单击查询,查看当前已设置的告警接收人。

6. 删除告警接收人。

在查询结果中,单击删除,可删除告警接收人。

10.4.4 管理事件日志存档

管理审计事件和原始日志的存档。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择存档管理页签, 如图 10-10: 存档管理页面所示。

图 10-10: 存档管理页面

市计策略 类型设置 告督设置 存档管理 导出管理				
审计类型: 全部 ▼ 归档类型: 全部 ▼ 发现时间: 起始时间 16	 →: 30 [^]/_∨ 至 終止时间 16 [^]/_∨: 30 [^]/_∨ 音响 			
文件名	摘要值	归档类型	创建时间	操作
OPS/2017-07-17/OPSOPS-20170717162815.gz	7f9d4fc7b56d140c5b72c17798203af6	事件归档	2017-07-17 16:28:15	下载
OPS/2017-07-17/OPSOPS-20170717162815.gz	76cdb2bad9582d23c1f6f4d868218d6c	日志归档	2017-07-17 16:28:15	下载
OPS/2017-07-17/OPSOPS-20170717162815.gz	69a23bbea7c48baa20edbede9a7af337	事件归档	2017-07-17 16:28:15	下载

- 4. 设置审计类型、归档类型和发现时间等查询条件,单击查询,查询归档信息。
- 5. 选择需要下载的存档文件,单击**下载**,可将存档文件保存到本地。

10.4.5 管理导出任务

在**审计查询**或**原始日志**页面,执行审计事件或日志导出后,可在导出管理页面对这些导出任务进行 管理。

- 1. 登录云盾安全中心。
- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择**导出管理**页签。
- 4. 查看已创建的导出任务,如图 10-11: 导出管理页面所示。

图 10-11: 导出管理页面

审计策略	类型设置	告警设置	存档管理	导出管理					
00200-0020			F		(1°47 MARI))	17948-4	40-4	49.1/-
2017-07-27 1	5:30:04		10	0302	审计事件得出	logType: logType: g: name: 全部理知 from: 1501054260000 to: 1501140660000	11954AD	log	Jact F 下载 删除
2017-07-27 1	5:29:20		10	0301	日志导出	logType: 1 soureld: 10155 年 name: 全部查询 form: 1501139700000 to: 1501140600000	್ರ ಕನನು	log	下载(翻除
								共有2条 ,每页5	訪:20条 ≪ < 1 > ≫

- 5. 单击下载,可将审计事件或日志文件下载到本地。
- 6. 单击删除,可删除该导出任务。

10.4.6 修改系统配置

通过设置安全审计的系统参数,可以配置系统单日最大报警次数及各类型原始日志的单日最大审计 量。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**安全审计 > 策略设置**。
- 3. 选择**系统设置**页签。
- 4. 选择设置项,单击编辑,如图 10-12: 系统设置所示。

图 10-12: 系统设置

审计策略	美型设置	情智设置	存枯管理	导出管理	系统设置
序号		说明			
1		每天	发送报警的最大》	大政	
2		每天	町汁原始日志量(总量:G8/天)	
3		每天	#计原始日志 量 ()	数据库:GB/天	
4		每天	前计原始日志量(主机 : GB/天)	
5		每天	前计原始日志量()	网络设备:GB/	天)
6		每天	副计原始日志量()	用户操作:GB/	天)
7		每天	単计原始日志量()	运缴操作:GB/	天)

5. 填写对应的参数值,单击确认。

11 系统管理

系统管理模块作为云盾安全中心不可或缺的部分,为安全管理员调整系统人员、配置提供了极大的便利。

系统管理主要包含四个部分:

- 阿里云账号管理:用于管理专有云云盾配套的阿里云账号。
- 云端同步:用于查看云盾情报库的更新方式及更新情况。
- 告警设置:用于配置各类安全事件、紧急信息等的告警方式以及联系人信息。
- 全局设置:用于配置云盾相关的网段信息,包括流量监控网段和区域网段两部分。

11.1 管理阿里云账号

操作步骤

- 1. 登录云盾安全中心。
- 定位到系统管理 > 阿里云账号管理页面,可以查看、修改系统绑定的阿里云账号信息,如图 11-1: 阿里云账号管理页面所示。

云盾中的资产均与阿里云账号绑定,请谨慎修改。

图 11-1: 阿里云账号管理页面

阿里云账号管理	里			
阿里云账号	用户ID	Access Key	Access Secret	操作
		and the second data	****	修改 详情

3. 单击修改,弹出修改对话框,信息修改后单击确定,完成修改,如图 11-2: 账号修改对话框所示。

图 11-2: 账号修改对话框

账号修改		\times
阿里云账号		
用户ID		
Access Key		
Access Secret		
	葰	定 取消

4. 单击**详情**,查看阿里云账号详细信息,包括许可到期时间、安骑士许可数目,如图 *11-3*: 账号详 情所示。这些信息均是通过配置的用户ID、Access Key信息获取。

图 11-3: 账号详情

帐号详情	\times
阿里云账号:	
用户ID:	
Access Key:	CONCERNMENT OF CONCERNMENT
Access Secret:	****
License到期时间:	2020-05-16
安骑士license数目:	0
	确定

11.2 云端同步

云端同步是将阿里公共云上的一些规则库、漏洞等安全信息同步到本地数据库。

云端同步是将阿里公共云上的0day规则库、漏扫漏洞库、漏洞主库、主机漏洞规则库、弱点扫描 插件库、弱点扫描规则库、安骑士Webshell检测规则库、安骑士漏洞管理 - Windows漏洞(系统补 丁)、安骑士漏洞管理 - Windows漏洞(规则文件)和安骑士漏洞管理 - 其它应急漏洞信息同步到 本地数据库。所同步的规则信息将应用于专有云云盾各对应功能模块中,确保在专有云环境中具备 与阿里云公共云同等的安全能力。

云端同步根据专有云环境的部署方式分为在线升级及离线升级包导入两种方式。

11.2.1 同步状态说明

云端同步列表中的数据是初始化的,只支持将阿里公共云上的各类规则库同步到本地数据库。 规则库信息与云端同步的频率和时间可以由管理员进行设置,可以是手动触发,也可以是自动触发;如果不设置,同步的频率将按照初始设置。

表 11-1: 同步状态说明表

状态	说明
待更新	云端有新版本规则库可以更新。
更新中	从云端下载并更新规则库。
更新完成	规则库更新完成。
更新失败	规则库更新失败。

11.2.2 刷新云端同步列表

操作步骤

- 1. 登录云盾安全中心。
- 定位到系统管理 > 云端同步页面,单击刷新,刷新云端同步列表,如图 11-4: 云端同步页面所示。

图 11-4: 云端同步页面

云端同步							
升级通道 👥 自动升级 👥						,	新 一键升级 升级包导入
规则库名称	当前版本号	升级时间	云鏡版本号	更新方式	更新频率	状态	操作
Oday规则库	0	2017-10-25 18:51:06	0	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
漏扫漏洞库	0	2017-10-25 18:51:11	0	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
遇词主库	0	2017-10-25 18:51:15	νб	自动	每天 01:00:00	● 更新失败	升级 回滾 设置 历史记录
主机漏洞规则库	0	2017-10-25 18:51:21	0	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
弱点归菌播件库	0	2017-10-25 18:51:26	0	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
弱点扫描规则库	0	2017-10-25 18:51:31	0	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
安骑士Webshell检测规则库	0	2017-10-25 19:33:00	0	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
安骑士濾洞管理 - Windows濡洞(系统补丁)	v62	2017-12-21 19:16:51	v62	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
安骑士濾洞管理 - Windows濾洞(规则文件)	v60	2017-12-21 19:16:51	v60	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
安骑士漏洞管理 - 其它应急漏洞	v64	2017-12-21 16:42:17	v64	自动	每天 01:00:00	● 更新完成	回滾 设置 历史记录
						共有10条 ,每页显示	: 20条 《 (1) »

刷新成功后,在云端同步页面,查看规则库在专有云环境中的当前版本号、云端版本号,以及更新方式、更新频率、状态等信息。选择规则库,单击当前版本号或云端版本号可查看规则库版本详情,如图 11-5:规则库版本详情所示。

图 11-5: 规则库版本详情

漏洞主库版本详情		\times
版本号: 更新内容:	v6_yundunCactusRule_yundunLeakageMain_V1.0 yundunLeakageMain发布	
		确定

11.2.3 设置更新方式

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**系统管理 > 云端同步**页面,选择规则库,单击设置。
- 3. 选择更新方式,如图 11-6: 规则库更新设置所示。
 - 图 11-6: 规则库更新设置

应急响应信息库	更新设置				\times
	更新方式:	● 自动	◎ 手动		
				确定	取消

4. 单击**确定**。

11.2.4 手动更新规则库

操作步骤

1. 登录云盾安全中心。

2. 定位到**系统管理 > 云端同步**页面。

3. 选择规则库,单击升级,将规则库信息从云端下载到版本库中。

说明:

单击云端同步页面右上方的一键升级,可以手动更新所有规则库。

11.2.5 回滚规则库

规则库更新完成后,可以通过回滚操作将规则库恢复至以前版本。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到系统管理 > 云端同步页面。
- 3. 选择规则库,单击回滚。
- 4. 在版本回滚对话框中,选择想要恢复到的规则库版本,如图 11-7: 版本回滚所示。

图 11-7: 版本回滚

版本回滚		Х
选择回滚版本	v61 •	
版本号	v61	
版本信息	安骑士漏洞管理 - Windows漏洞(系统补丁)-基线 包	
	确定	取消

5. 单击**确定**。

11.2.6 查看历史记录

操作步骤

1. 登录云盾安全中心。

- 2. 定位到系统管理 > 云端同步页面。
- 3. 选择规则库,单击历史记录,可以查看该规则库的同步记录,如图 11-8: 查看历史记录所示。

图 11-8: 查看历史记录

漏洞主库历史记录 🔹	返回上级列表	
更新版本号	更新时间	更新描述
νб	2017-12-08 15:30:07	yundunLeakageMain发布
		共有1条,每页显示:10条 ≪ < 1 > ≫

11.2.7 导入离线升级包

如果专有云环境无法与阿里云公共云连通,可以通过导入离线升级包的方式更新规则库。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到系统管理 > 云端同步页面。
- 3. 单击右上方的升级包导入。
- 在离线升级包对话框中,单击选择文件,选择已下载至本地的离线升级包,如图 11-9:导入离线 升级包所示。

图 11-9: 导入离线升级包

离线升级包		Х
选择文件 未选择任何文件 注意:目前只支持zip格式类型的文件		
	确定	取消

根据导入的离线升级包,云盾将完成相应规则库的更新,并在**云端同步**页面更新该规则库的状态。

5. 单击**确定**。

11.3 告警设置

告警设置功能包括设置告警联系人和按照不同的安全事件设置告警通知方式。当发生对应的安全事件时,系统自动上报告警,以便安全管理员了解系统发生的安全事件。

11.3.1 设置告警联系人

告警联系人是告警消息的接收人,告警消息的发送方式有手机短信和邮件。当监控数据满足报警规则时会发送告警信息给报警联系人。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到系统管理 > 告警设置 > 告警联系人页面,如图 11-10:告警联系人页面所示。

告警设置			
告誓设置 告警联系人			
			家加联系人
联系人姓名	手机	Email	操作
sdfs	1000000000	sdf@sdf.com	编辑 删除
yanmeng	15811096194	Balibaba-inc.com	编辑 目開歌
zhangsan	13000012568	abcd@albab.com	编辑 图象

图 11-10: 告警联系人页面

3. 单击添加联系人。

4. 填写联系人信息,单击确认,添加告警联系人。

添加后的告警联系人可以通过单击编辑或删除,对该联系人信息进行编辑或删除。

11.3.2 设置告警信息

告警设置可以对各种安全事件进行告警,告警方式包括手机和邮件。

- 1. 登录云盾安全中心。
- 2. 定位系统管理 > 告警设置 > 告警设置页面。
- 3. 在告警通知区域,为各种安全事件选择通知方式,如图 11-11:告警设置页面所示。

图 11-11: 告警设置页面

合管设置		
合营业区 合管业系人		
合管通知		
	① 金路	□ 金酒
党全	通知方式	
皇景史办-月地皇录 张号不在常用地登录	一 手机	二 邮件
派急导作告誓	通知方式	
阿克県会 阿克特県香華県。金原明6500以及社営営行等時辺方巡査同時は	○ #%	() 第4
利用行力 主式法認可持00x8行力: 新聞記言有単属書類的所力	○ 手机	□ ¥n
解结成功 累高管试验解被码最短点机,并通过一系列管试后盘起成功	○ #4.) 第4

4. 单击确认,完成设置。

11.4 全局设置

云盾安全中心提供全局设置,供安全管理员对云盾流量安全监控模块的网段范围以及安骑士模块上 报检测的区域进行设置。

说明:

流量安全监控模块的采集网段设置和区域设置中如果配置同一网段,则区域信息必须一致。

11.4.1 流量采集网段设置

网段设置主要针对流量安全监控模块进行网段配置,并且支持更改监控的网段范围,方便安全管理 员根据需求调整监控的网段。配置的监控网段仅对所属区域机房生效。



网段设置更改后立即对流量监控生效,不需要安全管理员进行其他操作。

11.4.1.1 添加流量采集网段

- 1. 登录云盾安全中心。
- 2. 定位到系统管理 > 全局设置 > 流量采集网段设置页面。
- 3. 单击添加,弹出添加监控网段对话框,如图 11-12:添加监控网段对话框所示。

图 11-12: 添加监控网段对话框

添加监控网段	×
网段 区域	请输入监控网段,例如:10.158.192.0/24
	确定 取消

- 4. 设置监控网段参数。
 - 填写网段。

送明 :
所填写的网段必须是合法网段,并且不允许重复添加。

- 选择所属区域。
- 5. 单击确定,完成添加。

11.4.1.2 管理流量采集网段

- 1. 登录云盾安全中心。
- 2. 定位到**系统管理 > 全局设置 > 流量采集网段设置**页面。
- 3. 选择区域,输入查询网段,单击**查询**,查看流量采集网段信息,如图 11-13: 流量采集网段所示。

图 11-13: 流量采集网段

区域: 全部	▼ 輸入查询网段 查询	添加
网般	区域	操作
1.2.3.0/24	cn-neimeng-env10-d01	修改 删除
10.10.150.0/24	cn-neimeng-env10-d01	修改 删除
42.36.0.0/16	cn-neimeng-env10-d01	修改 删除
192.168.1.0/24	cn-neimeng-env10-d01	修改 删除
192.168.197.0/24	cn-neimeng-env10-d01	修改 删除

- 4. 管理流量采集网段。
 - 单击修改,在修改网段对话框中修改所属区域,单击确定,修改流量采集网段所属区域。
 - 单击删除,可删除该流量采集网段。

11.4.2 区域设置

区域设置主要针对不同机房安骑士客户端的区域检测,配置后,所属区域对应网段下的安骑士主机 上报后,可以自动检测匹配对应的机房。

区域设置支持更改已配置网段的所属区域,但是更改后必须在资产总览中批量修改对应网段资产的 区域。

11.4.2.1 添加区域网段

- 1. 登录云盾安全中心。
- 2. 定位到系统管理 > 全局设置 > 区域设置页面。
- 3. 单击添加,弹出添加网段对话框,如图 11-14:添加网段对话框所示。

图 11-14: 添加网段对话框

添加网段		×
网段 区域	请输入网段,例如:10.158.192.0/24	
	8	取消

- 4. 设置网段参数。
 - 填写网段。



- 选择所属区域。
- 5. 单击确定,完成添加。

11.4.2.2 管理区域网段

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到**系统管理 > 全局设置 > 区域设置**页面。
- 3. 选择区域,输入查询网段,单击查询,查看区域网段信息,如图 11-15: 区域设置页面所示。

图 11-15: 区域设置页面

区域	网段		操作
cn-hangzhou-env6-d01	172.10.1.0/24	修改	創除
		共有1条, 每页显示: 10条 " (1)	×

4. 管理区域网段。

- 单击修改,在修改网段对话框中修改所属区域,单击确定,修改区域网段信息。
- 单击删除,删除该区域网段信息。

11.4.3 配置白名单

操作步骤

- 1. 定位到**系统管理 > 全局设置 > 白名单设置**。
- 2. 单击添加。
- 3. 在添加白名单对话框中,设置白名单参数,如图 11-16:添加白名单对话框所示。

图 11-16: 添加白名单对话框

添加白名单			\times
源IP	请输入IP/网段		
目的IP	请输入IP/网段		
用户名	请输入用户名,且用户名长度不超过64位		
 类型	主机暴力破解白名单	v	
		确定	取消

参数	说明
源IP	源IP/网段。
目的IP	目的IP/网段。
用户名	添加白名单记录的用户名称
类型	 bwaf源ip白名单:符合该白名单的流量将不会被检测。 主机暴力破解白名单:符合该白名单中的登录行为将不进行暴力破解检测。

参数	说明
	• 应用攻击白名单:符合该白名单中的疑似应用攻击行为将不 会被检测。

4. 单击**确认**。

白名单添加成功后,单击删除,可删除已不需要的白名单。

12 可选安全产品

12.1 DDoS防护

DDoS(Distributed Denial of Service),即分布式拒绝服务。DDoS攻击指借助于客户/服务器技术,将多个计算机联合起来作为攻击平台,对一个或多个目标发动DDoS攻击,从而成倍地提高拒绝服务攻击的威力。

常见的DDoS攻击包括以下几类:

- 网络层攻击:比较典型的攻击类型是UDP反射攻击,例如:NTP Flood攻击,这类攻击主要利用 大流量拥塞被攻击者的网络带宽,导致被攻击者的业务无法正常响应客户访问。
- 传输层攻击:比较典型的攻击类型包括SYN Flood攻击、连接数攻击等,这类攻击通过占用服务 器的连接池资源从而达到拒绝服务的目的。
- **会话层攻击**:比较典型的攻击类型是SSL连接攻击,这类攻击占用服务器的SSL会话资源从而达 到拒绝服务的目的。
- **应用层攻击**:比较典型的攻击类型包括DNS flood攻击、HTTP flood攻击、游戏假人攻击等,这 类攻击占用服务器的应用处理资源极大的消耗服务器处理性能从而达到拒绝服务的目的。

云盾可以对攻击流量进行牵引、清洗和回注,提供对DDoS攻击的防御,保证业务正常进行。

12.1.1 查看DDoS事件

云盾在进行流量清洗或流量清洗结束,会上报安全事件到云盾安全中心。通过本章节可以查看到DDoS事件。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 网络防护,选择DDoS事件页签。

进入DDoS事件列表,如图 12-1: DDoS事件页面所示。

图 12-1: DDoS事件页面

DDoS防护											
DDoS事件 DDoS设置											
所屬区域: 全部	▼ 请输入IP地址		请输入触发原因	状态: 全部	▼ 开始时间:	起始时间		至	终止时间		
查询											
开始时间	结束时间	触发原因	对外服务IP	所属用户	所属区域		状态				攝作
2018-01-09 19:06:15		pps,qps	10		cn-hangzhou-env6-i	d01	清洗中		取満清洗	流量分析	查看流量
2018-01-09 18:32:55		pps,qps	10		cn-hangzhou-env6-	d01	清洗中		取満清洗!	流量分析	查看流量
2018-01-09 16:52:50		pps,qps	10		cn-hangzhou-env6-i	d01	清洗中		取消清洗	流量分析	查看流量
2018-01-09 16:26:55	2018-01-09 16:58:00	bps,pps	10		cn-hangzhou-env6-	d01	清洗结束			流量分析	查看流量
2018-01-09 16:15:40	2018-01-09 20:34:24	pps,qps	10		cn-hangzhou-env6-i	d01	清洗结束			流量分析	查看流量

3. 设置查询条件,单击查询。

可根据查询条件返回满足条件的DDoS事件信息。

信息列	说明				
触发原因	示DDoS攻击流量中哪一指标超过了设置的预警阈值。				
对外服务IP	表示受到DDoS攻击的IP。				
状态	 清洗中:表示正在进行流量清洗。 清洗结束:表示流量清洗已经结束。 				
操作	 取消清洗:手动停止流量清洗。 流量分析:查看DDoS事件中流量协议和Top10主机。 查看流量:查看预警阈值和流量图。 				

- 4. 查看和分析DDoS事件。
 - 单击查看流量,查看对应IP当前的设置阈值及流量图,如图 12-2: 流量视图所示。

图 12-2: 流量视图



• 单击**流量分析**,查看当前攻击事件的流量成分、Top10攻击机分析,如图 12-3:流量分析页面所示。

图 12-3: 流量分析页面



12.1.2 DDoS防护策略

DDoS流量报警阈值即当访问该IP的流量达到阈值后触发流量报警。IP的阈值设置通常以流量作为依据,当流量过大时,表示可能受到DDoS攻击。

阈值一般建议设置为比流量的高峰期值稍大即可。

云盾支持全局阈值设置、网段阈值设置和单个IP地址阈值设置三种方式:

- 全局阈值:全局阈值无法添加,默认值在服务初始化时通过导入实现。
- **网段阈值**:根据网段的流量,设置待设定网段的报警阈值。网段阈值设置方式相对全局阈值能更 精准地设置对应网段的报警阈值。
- 单个IP地址阈值:根据每个IP地址的流量,分别设置对应的报警阈值。单个IP地址阈值的设置方 式相对网段阈值能更精准的设置每个IP的报警阈值。

12.1.2.1 设置预警阈值

单独对一个网段或一个IP设置阈值时,以该阈值为准触发DDoS检测,否则按照全局阈值触发DDoS检测。

操作步骤

1. 登录云盾安全中心。

2. 定位到网络安全 > 网络防护,单击DDoS设置。

进入DDoS设置页面,如图 12-4: 阈值列表所示。

图 12-4: 阈值列表

DDoS事件 DDoS设置						
						新建防护策略
对外服务IP	所属用户	区域	预警流速(Mbps)	预警包速(pps)	预曾HTTP请求速率(qps)	操作
192.1	yundun_test02	cn-hangzhou-env6-d01	1	1	51	修改 删除
10.36		cn-hangzhou-env6-d01	1	1	51	修改 删除
10.36		cn-hangzhou-env6-d01	100	100	100	修改 删除
128.0		cn-hangzhou-env6-d01	500	500	100000	修改
192.1	yundun_test02	cn-hangzhou-env6-d01	1	1	51	修改 删除
10.36		cn-hangzhou-env6-d01	2000	100000	60	修改 删除
default		cn-hangzhou-env6-d01	80000	0	0	修改

3. 单击新增防护策略。

4. 在新增防护策略对话框中,设置预警参数,如图 12-5: 新增防护策略对话框所示。

图 12-5: 新增防护策略对话框

新增防护策略		\times
IP地址	192.168.1.100]
预警流速	100	Mbps
预警包速	20000	pps
预警HTTP请求速率	100000	dba
	Q	靛取消

参数	说明
IP地址	设置预警的IP地址或网段。
	说明 : 添加阈值时,务必确认对应的网段已在流量采集网段设置中添加。
预警流速	设置机房中带宽报警阈值。当机房入+出流量速率达到该值 时,即触发DDoS检测。一般根据业务实际使用带宽值设 置,比峰值略大即可,建议阈值至少设置为100 Mbps以上。 带宽单位为:Mbps(兆比特 / 秒)
预警包速	设置机房包速率报警阈值。当机房入+出包速率达到该值 时,即触发DDoS检测。一般根据业务实际使用包速率设 置,比峰值略大即可,建议阈值至少设置为20000 pps以上。 包速率单位为: pps(包个数 / 秒)
预警HTTP请求速率	设置机房主机收到的HTTP请求速率报警阈值。当机房 入+出HTTP请求速率达到该值时,即触发DDoS检测。一般根 据业务实际情况设置,比峰值略大即可,建议阈值至少设置 为100000 qps以上。 HTTP请求速率单位为:qps(请求个数 / 秒)

5. 单击**确定**。

12.1.2.2 管理预警阈值

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 网络防护,单击DDoS设置。
- 3. 管理已添加的防护策略。
 - 单击修改,在弹出的修改防护策略的对话框中,输入对应的阈值后单击确定,修改预警阈 值。
 - 单击删除,删除该预警阈值。



系统默认阈值无法删除。

12.2 云防火墙

云防火墙是一款针对云环境的防火墙安全产品,主要解决云上业务快速变化带来的安全边界模糊甚 至无法定义的问题。云防火墙模块能够帮助安全管理员完成专有云环境中云服务器的业务分区和隔 离策略的部署。

12.2.1 开始之前

当您需要配置云防火墙前,需要角色授权。

- 1. 创建云防火墙服务对应的Ram角色,具体请参见《用户指南》中RAM管理一节。
- 定位到云管控中心 > 云基础产品 > 云盾控制台,单击立即授权,把用户所属部门添加到已授权 部门中。

在进行云防火墙配置之前,安全管理员需要根据实际业务情况准备以下规划信息:

- 所需业务区,例如,测试区、开发区等。
- 每个业务区所需的服务器角色,例如,Web应用(Web)、数据库(DB)等。
- 确定ECS云服务器与业务区及服务器角色组之间的对应关系,即每台ECS云服务器需要被划分至 哪个业务区以及角色分组中。

12.2.2 拓扑图图例说明

图例

在云防火墙拓扑图中,通过以下图形和颜色标识拓扑图中的各个要素信息。

发布 湔	添加策略 新建业务 一键全	通 一键恢复 导出 智	能搜索 图列 🔺
业务区状态	业务区类型	流量状态	流量方向
➡ 未发布	固定业务区	— 已定义放行策略)从上到下
② 拦截模式	临时业务区	—— 不可定义策略	(从下到上
◎ 观察模式		— 待定义策略	
🛞 发布失败			
🛷 发布中			

■ 说明:

在云防火墙拓扑图中,将鼠标移至流量线上可以通过观察虚线的流动情况来判断流量的访问方向,虚线的流动方向即是该流量的访问方向。

流量线筛选

云防火墙拓扑图提供多种筛选方式,通过隐藏/显示部分流量线的方式帮助您在拓扑图中找到您需要 重点观察的流量线。

● 业务区之间 ● 业务区之内 ● 外网入方向 ● 出方向 ● ある	▲ 121xB ▼
☞ 绿色流量线	1天
☑ 红色流量线	1个月
● 灰色流量线	
● 角色组名	
	-
端口: 多个以逗号隔开 确定	

• 流量线类型筛选:

勾选或取消**业务区之间、业务区之内、外网入方向**和**出方向**,可设置是否在拓扑图中显示相应类型的流量线。

• 流量线颜色筛选:

单击**更多**,勾选或取消**绿色流量线、红色流量线**或**灰色流量线**,可设置是否在拓扑图中显示相应 状态的流量线。

在端口中输入端口号,单击确定,自定义设置在拓扑图中不显示与所输入端口相关的流量线。

在更多下拉菜单中勾选角色组名,可在拓扑图中的业务分区内显示具体的角色组名称。

• 时间范围筛选:

单击时间范围筛选框,选择时间范围,在拓扑图中将显示指定时间范围内的流量线。

展现方式

云防火墙拓扑图提供多种展现方式,您可以根据实际情况自由切换展现方式。



・ 业务区展现方式:

单击相应的业务区展现方式按钮即可切换展现方式。

东西向:业务区以东西向的方式进行排列展示。在业务区较多的情况下,可以单击拓扑图左侧或右侧的箭头查看其它业务区;将鼠标移至业务区,单击业务区下方的左移、右移箭头可以调整业务区的排列顺序。

通过东西向的展现方式,可以帮助您集中观察部分业务区的关联流量信息。

- 列表:在拓扑图中展示所有业务区。通过列表的展现方式,可以帮助您全局地了解所有业务
 区的关联流量信息。
- 流量线展现粒度:

单击相应的流量线展现粒度按钮即可切换流量线的展现粒度,包括**业务区、角色组、主机**三种粒度,您可以根据实际情况选择拓扑图中流量线的展现粒度。

12.2.3 建立业务区

在云防火墙控制台中新建业务区。

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 选择需要管理的云服务器所属的区域和专有网络(VPC),如图 12-6: 选择区域及网络所示。

图 12-6: 选择区域及网络

云防火墙拓扑图			
地域:	cn-hangzhou-	网络:	test_vpc_

- 4. 单击新建业务区,如图 12-7:新建业务区所示。
 - 图 12-7: 新建业务区

您在cn-hangzhou 地域的 vpc环境下,共有 台云服务器ECS
您当前还没有业务区,请新建业务区



如果在该VPC环境中已创建过业务分区,请在页面上方的菜单栏中单击新建业务。

5. 填写业务区名称,选择业务区标签。如图 12-8: 创建业务区所示。

图 12-8: 创建业务区

新建业务区	×
业务区名称:	7
建议名字具有较高的识别性,长度为2-128个字母、符号或汉字。 您当前已有1个业务区。	_
业务区标签: 测试 ▼	
	取消 确定

6. 单击**确定**。

12.2.4 导入ECS云服务器

在业务区中导入ECS云服务器。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在**云防火墙拓扑图**页面,选择需要管理的业务区所属的区域,以及所属专有网络(VPC)的名称。
- 4. 将鼠标移至已创建的业务区,显示操作按钮,如图 12-9: 操作按钮所示。

图 12-9: 操作按钮


- 5. 单击添加资产按钮 👝 ,打开添加资产窗口。
- (可选)设置搜索条件,单击搜索。
 通过设置公网IP、实例名和标签搜索条件,可以快速搜索需要的服务器。
- 7. 选择需要添加的服务器,单击**立即添加**,如图 12-10:添加资产所示。

图 12-10: 添加资产

添加	资产					×
当前」	业务区共有3台服务器。	+= /\-		40.00		
WP:	义例名:	标签:		喪業		
	服务器ID/实例名		公/私网IP	协议/端口/进程		
	i-5v	rzZ	/192.168.77.20	tcp/22/sshd、tcp/	25/sendmail.se	
	全选		共有1条,	每页显示:20条	« < 1 >	20-
共选持	译 1台服务器 立即添加					

12.2.5 建立角色组,将已导入的ECS云服务器分组

在云防火墙业务区中建立角色组,并将已导入的ECS云服务器进行角色分组。

12.2.5.1 将已明确角色的ECS云服务器进行分组

建立角色组,并将已导入的具有明确角色的ECS云服务器进行分组。

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在**云防火墙拓扑图**页面,选择需要管理的业务区所属的区域,以及所属专有网络(VPC)的名称。
- 4. 将鼠标移至已创建的业务区,显示操作按钮,如图 12-11:操作按钮所示。

图 12-11: 操作按钮



- 5. 单击用户管理按钮 👝 ,打开角色管理页面。
- 6. 单击源角色组旁的添加角色组按钮(+),新建角色组,如图 12-12:新建角色组所示。

图 12-12: 新建角色组

1 定义	角色				^
源IP	\$	请输入源IP搜索	搜索	请输入角色	组名 确定 取消 添加角色组
访问源				访问目的	源角色组

- 7. 填写角色组名,单击确定。
- 8. 根据访问源中的ECS云服务器信息,为ECS云服务器选择已创建的源角色组,如图 *12-13*: 分配 角色组所示。

图 12-13: 分配角色组

角色管理 (测试-测试)		
1 定义角色		^
源IP ◆ 请输入源IP搜索 搜索		
访问源	访问目的	源角色组
昵称: tcpnetstatin 进程: tcp/AliYunDun 系统: centos 服务: 22	(公) /(私) (tcp/80)	

12.2.5.2 将未明确角色的ECS云服务器进行分组

对于未明确角色的ECS云服务器,参考以下操作步骤使用云防火墙提供的流量可视化功能,明确每 一台ECS云服务器的角色。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在**云防火墙拓扑图**页面,选择需要管理的云服务器所属的区域,以及所属专有网络(VPC)的名称。
- 4. 简化拓扑网络。
 - 流量线范围筛选:

✔ 业务区之间	🕑 业务区之内 📃 外网入方向	□ 阿里云入方向 □ 出方向 更多▲	1258 ¥
		✔ 绿色流量线	
		✔ 红色流量线	
		✔ 灰色流量线	
		▲ 角色组名	
		送口: 友太川海見原王 · 梅安	
		·····································	

根据实际业务情况在拓扑图上方仅勾选需要显示的流量线,从而简化拓扑图。

您也可以单击**更多**,勾选是否显示特定类型的流量线,或者自定义不显示特定端口的流量 线。

同时,您还可以单击时间维度选择所显示的流量线的时间范围。

智能搜索:

智能搜索	×
□ 规则名称 规则条件 🞯	是否显示
□ 选择业务区 ▼ 选择角色组 ▼ ip地址 端口 关键字	
☞ 缺省规则 其他业务区-其他角色组	
保存并执行 添加规则 ?	

通过设定搜索规则显示或不显示某个业务区或某个角色组的特定流量线。



智能搜索提供了强大的搜索规则功能,来实现过滤不相关流量信息的显示效果。智能搜索规则可以组合执行,采用自上而下的匹配顺序;每条规则都可单独设定是否显示符合规则条件的流量线。

- 1. 单击拓扑图右上方的智能搜索。
- 2. 单击添加规则,设置智能搜索规则,如图 12-14: 自定义搜索规则所示。

图 12-14: 自定义搜索规则

□ 规则名称	规则条件 🛛	是否显示
₹ 2	ab游戏开发线上 \$ web \$ ip地址 80 关键字	
□ 1	ab游戏开发线上 ◆ 选择角色组 ◆ ip地址 80 关键字	0
☑ 缺省规则	其他业务区-其他角色组	0
保存并执行	添加规则	

- 最多可以定义10条搜索规则,并且系统默认有一条缺省规则。
- 通过左侧的勾选框决定搜索规则是否生效,缺省规则无法取消勾选。
- 3. 勾选需要使用的智能搜索规则,单击保存并执行。

在拓扑图中,单击某台服务器,可以查看该服务器的相关信息及与该服务器相关的流量线,其它的流量线信息将不显示。

- 5. 在业务区中,将鼠标悬停在ECS云服务器的节点上,查看该ECS云服务器的服务器信息,如图 12-15: 查看服务器信息所示。
 - 图 12-15: 查看服务器信息



6. 单击ECS云服务器节点,查看该ECS云服务器与其他服务器之间的访问关系,如图 12-16: 查看 服务器之间访问关系所示。

图 12-16: 查看服务器之间访问关系



7. 在角色管理页面中,通过查看本业务区所有ECS资产的服务器信息、及ECS资产与其他服务器的访问关系,判断该ECS资产的应属角色组,如图 12-17:通过角色管理查看服务器之间访问关系所示。

图 12-17: 通过角色管理查看服务器之间访问关系

((**	角色管理(艾客测试-勿动-线上)		×
	1 定义角色 源IP ◆ 请输入源IP搜索 搜索		^
	访问源	访问目的	源角色组 🕒
Service_70-701	(公) / 10.30.55.233(私) 昵称: aike_buy_centeos 进程: tcp/ssh、tcp/N/A、tcp/python、tcp/cur I、t 系统: centos 服务: 22,25,70,701	 (上) / 10.30.56.37(私) (tcp/22、 tc (上) / 10.80.52.20(私) (tcp/801、 tcp/ (上) / 10.31.145.128(私) (tcp/80、 t (L) / 10.30.51.102(私) (tcp/80、 t 	service_70-7(\$
service_60-801	(公) / 10.30.56.37(私) 昵称: service-艾客测试 进程: tcp/python, tcp/ssh、tcp/AliYunDun 系统: centos 服务: 22,25,80	(公) / 10.30.55.14(私) (tcp/9091) (公) / 10.30.54.250(私) (tcp/9091) 1(公) / 10.30.51.102(私) (tcp/22) (一(私) (tcp/80) 更多	service_80-8(\$
service_monitor web_10001 I 管理p	(公)/10.31.154.192(私) 昵称: hht_test 进程: tcp/wget, tcp/sshd、tcp/python、tcp/Ali Y 系统: centos 服务: 22,25	 、) /(私) (tcp/80) (公) / 10.31.145.128(私) (tcp/22) /(私) (tcp/80) 、) /(私) (tcp/80) 	service_moni \$

12.2.6 审核流量(部署访问控制策略)

在云防火墙控制台中,逐一审核流量的合法性、部署访问控制策略。

背景信息

只要业务区没有发布,在该业务区上的所有操作、策略部署并不会真实发布,更不会影响实际业务。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在**云防火墙拓扑图**页面,选择需要部署的业务区所属的区域,以及所属专有网络(VPC)的名称。
- 4. 在业务区中查看流量线条。

未审核流量线默认都是红色线条,需要逐条确认该流量的合法性,如图 12-18: 审核流量线条所示。

图 12-18: 审核流量线条



5. (推荐)通过流量线审核,定义相应的白名单访问控制策略。

送明 :	
审核通过后的流量将会显示为绿色。	

- a) 单击红色流量线。
- b) 对该流量线进行放行或拒绝操作,如图 12-19: 对流量线定义访问控制策略所示。

图 12-19: 对流量线定义访问控制策略

流量线:	.wi-84					
流量						
目的端口/	协议	流量来源		是否有策略		操作
22/tcp		47.86-08.187		无策略		放行 拒 绝
放行策略						
访问源	访问目的	网卡类型	端口范围(2	策略备注	操作
暂无策略						

6. 手动添加访问策略。

说明:

建议通过对拓扑图中可视化的具体流量线操作的方式定义访问控制策略,参见步骤5。

在角色管理页面中的建立策略区域,单击添加,直接添加相应的访问控制策略,如图 12-20:
 添加访问控制策略所示。

图 12-20: 添加访问控制策略

2 建立策略					^
访问源	访问目的	网卡类型	端口范围 🛛	策略备注	操作
业务区 abc	业务区 def	内网	1/55		删除
业务区 def	业务区 abc	内网	44/88		删除
业务区 ♦ 请选择角色 ♦	请选择 ♦	外网 🗘	端口范围	策略备注	保存 取消
十添加 🛛					

• 单击拓扑图右上方的**添加策略**,手动添加访问控制策略,如图 12-21: 手动添加访问控制策略所示。

图 12-21: 手动添加访问控制策略

添加策略							\times
访问源类型: 业务区		•	访问源业务区: 请选择	•	访问源角色组: 请选择		•
访问日的突然	₩:	۳					
网卡类型:	内网	•					
端口范围:	请输入端口范围		取值范围从1到65535;填写格式效	ם"1/20	0"、"20/20"。		
策略备注:	请输入策略备注						
						确定	取消

12.2.7 发布业务区(下发访问控制策略)

完成访问控制策略部署后,将该业务区进行发布。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在**云防火墙拓扑图**页面,选择您想要发布的业务区所属的区域,以及所属专有网络(VPC)的名称。
- 4. 单击页面右上方的发布/生效/回滚。
- 5. 选择发布模式,选择需要发布的业务区,单击**发布**。



• 发布观察模式:

发布观察	と 模式 发布拦截模式	t	刷新
1. 有关眼 2. 拦截構 3. 您有1	統量线的业务区必须一步 試不可以回退到观察模式 台ECS未加入到云防火墙	超发布,不能单独发布。 式,拦截模式可以使用一键全通。 韵固定业务区的角色组中,开启拦截模式后,可能会影响您的业务。不建议开启拦截	莫式。
✔ 昵称	Ŗ	状态	操作
 测试 	1—区-测试	无需发布	-
2	发布 0		

在尚不完全确定该业务区的策略配置是否合理时,建议选择**发布观察模式**。在观察模式 下,云防火墙中仅模拟流量与访问控制策略,不会对流量进行真实阻断。

业务区发布为观察模式后,您可以在一段时间后继续观察拓扑图中是否出现其它未被放行的 正常业务流量线,并配置相应的访问控制策略。

• 发布拦截模式:

选择**发布拦截模式**,云防火墙将根据业务区中所有基于流量线、服务器或角色组配置的访问 控制策略自动生成安全组规则。拦截模式发布成功后,所有不在白名单策略定义的流量都会 被拦截。

送 说明:

为了避免ECS实例原先所属的安全组的规则影响云防火墙的访问控制规则的效果,在将所有业务区以拦截模式发布后,您需要将所有ECS实例从原先的安全组中移出,在云防火墙中配置访问规则才能真正生效。

后续操作

在业务区以拦截模式发布后,如果所配置的访问控制策略导致正常业务被中断,您可以使用一键全 通功能实现在特殊情况下为某个业务区提供临时性放行策略,从而为您争取更多的排查时间。

关于一键全通功能的详细说明,请参见临时使用一键全通功能。

12.2.8 临时使用一键全通功能

背景信息

业务区发布后,如果出现因防火墙策略配置导致的业务中断,可以参考以下操作步骤使用云防火墙的一键全通功能,为对应的业务区提供临时性放行策略的机制,从而争取更多的排查时间。

操作步骤

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在云防火墙拓扑图页面,选择相关业务区所属的区域,以及所属专有网络(VPC)的名称。
- 4. 单击页面右上方的一键全通。
- 5. 勾选需要一键全通的业务区,单击确定,如图 12-22:一键全通所示。

图 12-22: 一键全通

一键全通
慎重提示:如果该业务开通"一键全通"功能,当前业务区上所配置的安全拦截策略将暂时失效,这将 导致外网可以访问此业务区的所有服务器,并对您的业务造成一定的安全隐患。直到您执行"一键恢 复"后,之前的相关安全拦截策略才会重新生效,建议您慎重开启一键全通。
1. 一键全通只针对拦截模式的业务区。 2. 一键全通后,系统将会为出入该业务区的全部流量,执行临时放行策略。
请选择要一键全通的业务区:
□ 所有业务区
取消 确定

 问题排查完成后,单击云防火墙拓扑图页面右上方的一键恢复,自动删除一键全通功能所增加的 临时放行策略,恢复到业务区原有的策略配置。

12.2.9 管理云防火墙所有资源

安全管理员也可以在云防火墙控制台中的**资源列表**页面,对业务区、角色组、以及ECS云服务器资源进行管理。

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在云防火墙拓扑图页面,单击左上方的返回资源列表,如图 12-23: 返回资源列表所示。

图 12-23: 返回资源列表



- 4. 选择需要管理的资源所属的区域,以及所属专有网络(VPC)的名称。
- 5. 在资源列表页面,管理云防火墙相关资源,如图 12-24:管理云防火墙资源所示。

图 12-24: 管理云防火墙资源

云眉 • 云防火墙	资源列表							
拓扑图	① 在此修改或增加的动作需要发布以后生	98.						\times
资源列表	地域: cn-hangzhou 网络: vp	¢	选择业务区	选择角色组 •	IP •	请输入IP进行搜索		搬表
策略管理					选择搜	款对象是IP或端口		
	新有资源 4台 + 新建业务区	■ 乙酸芳香口/虫外名 公/私用印 最常用进程				业务区	角色 组	操作
	App 0台× 副陰後角色組 DB 1台	 minus winus wich k i-3 minus wich k i-4 minus wich k i-192.168.1.32 NA/8094, rpcbind/111, rpc.mountd/50340, rp i-192.168.1.32 NA/46200, sshd/22, java/32000, dockerd/237 	c.mountd/40044, 77、dockerd/7946	rpc.mountd/35034、	N/A/2049、	doctest- 測试	DB	更换 角色 组
	test2 0给 test2 0给 Web 3给	-/192.168.1.206				doctest- 測试	Web	更换 角色 组
Ξ		i-3pc/192.168.1.55				doctest- 測试	Web	更换 角色 组
		l-3pu				doctest- 測成	Web	更换 角色 组
		■ 更為在色祖 批量更終角色组		共有4条,每	ē页显示 20	▼ ∰ ≪ <	1 >	>

送明:

在此页面进行的增加、修改的动作都需要发布相关业务区后才会生效。

12.2.10 管理访问控制策略

业务区发布后,安全管理员可以在云防火墙控制台中的**策略管理**页面,查看并管理已创建的访问控制策略。

- 1. 登录云盾安全中心。
- 2. 定位到网络安全 > 云防火墙,进入云防火墙控制台。
- 3. 在云防火墙拓扑图页面,单击左上方的返回资源列表。
- 4. 单击**策略管理**。
- 5. 在策略管理页面,选择想要查看或管理的策略所属的区域,以及所属专有网络(VPC)的名称。
- 6. 管理访问控制策略,如图 12-25:管理访问控制策略所示。

图 12-25: 管理访问控制策略

云眉 • 云防火墙	策略管理								
拓扑面	 在此修改或增加的动作需要发布以后生效。 					\times			
资源列表	地球: cn-hangzhou musi min 网络: vpm	Right: cn-hangzhou muni mu Right: vp-mini							
領地管理	源角色组: 目的角色组:	龍衆				十派加策略			
	□ 访问源角色组	访问目的角色组	协议/脑口	公私网	状态(全部) +	摄作			
	 doctest-辨式 D6 	doctest-現紀 Web	tcp/1/1	内网	未应用	809			
	□ doctest-例此 test1	doctest-测试 test2	tcp/1/10000	内网	未应用	899			
	B 899				共有2条,每页显示20 🔻 条	« < 1 > »			



说明:

在此页面进行的增加、修改的动作都需要发布相关业务区后才会生效。

- 查看或删除该网络区域内已配置的访问控制策略。
- 单击添加策略,手动添加访问控制策略。

送 说明:

建议通过对云防火墙拓扑图中可视化的具体流量线操作的方式定义访问控制策略。

策略项	说明
访问源	 访问源类型为业务区:设置访问源业务区和角色组。 访问源类型为IP地址或网段:设置访问源IP段。
访问目的	 访问目的类型为业务区:设置访问目的业务区和角色组。 访问目的类型为IP地址或网段:设置访问目的IP段。
网卡类型	设置网卡类型,即策略对哪个网卡的流量生效。
端口范围	设置端口范围,即策略对哪些端口的流量生效。
策略备注	设置策略备注。

12.3 堡垒机

云盾堡垒机为云服务器的运维提供完整的审计回放和权限控制服务。基于账号(Account)、认证(Authentication)、授权(Authorization)、审计(Audit)的AAAA统一管理方案,通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能,增强运维管理的安全性。

云盾堡垒机符合各类法令法规的要求,包括等级保护、银监会、证监会、PCI安全标准委员会、企业内控管理等相关政策规定要求。

12.3.1 堡垒机系统部署

堡垒机系统通过镜像方式部署在专有云Enterprise版平台上的ECS云服务器中。

操作步骤

1. 登录Apsara Stack控制台。



部署堡垒机系统需要使用具有相关资源权限的用户进行操作。

- 2. 定位到云管控中心 > 云基础产品 > 云服务器,选择实例页签。
- 3. 单击创建实例,进入创建云服务器ECS页面,创建云盾堡垒机系统服务器。
 - a) 设置区域、配置基本配置、网络等信息。

图 12-26: 设置ECS实例配置属性

♀ 区域	区域	cn-qiandaohu-sg-d01	0		
	*可用区	可用区a		•	0
② 基本配置	*部门	yundun		•	
	*项目	yundun		•	
④ 网络	* 网络类型	经典网络	专有网络		
		yundun/vpc-	5	•	yundun_sw1/vsw 35
	*安全组	yundun_sg		•	
	配置私网IP:	当前虚拟交换机网段为	: 172.16.0.0/16		

b) 单击**请选择实例规格**,选择ECS实例规格。

建议规格如下:

- CPU:4核
- 内存:8G
- c)选择公共镜像,下拉菜单中选择堡垒机镜像,并选择对应的版本。

d) 配置40G的系统盘和800G的数据盘。

说明 : 数据盘至少需要	要100G,否则	服务无法启动	动。			
₿存储	* 系统盘	高效磁盘	•	40	GB	请输入40-500
	数据盘	高效磁盘 田増加一块	▼	800	GB	□ 随实例释放 ①

e) 填写服务器密码、实例名称,单击创建,创建云盾堡垒机系统ECS实例。

12.3.2 admin管理员快速配置指南

12.3.2.1 登录云盾堡垒机系统

前提条件

- 请确认您所使用的客户端能够正常访问云盾堡垒机系统。
- 请确认您已经从云盾堡垒机系统部署人员处获得云盾堡垒机系统的访问地址。
- 请确认您已经从云盾堡垒机系统部署人员处获得超级管理员(admin)的初始密码。

- 1. 打开Chrome浏览器。
- 2. 在地址栏中,输入https://云盾堡垒机系统的访问地址,按回车键(Enter),进入系统登录页面,如图 12-27: 云盾堡垒机系统登录页面所示。

图 12-27: 云盾堡垒机系统登录页面

こう 阿里云 云盾堡垒机系统	
密码 短信口令 手机APP口令	
▲ 用户名	
▶ 密码	
验证码	
登录	

- 3. 在云盾堡垒机系统登录页面,输入超级管理员用户名(admin)、密码及验证码。
- 4. 单击**登录**。

📋 说明 :

首次登录成功后,管理员必须修改密码。

12.3.2.2 快速配置

云盾堡垒机系统采用集中配置模式,将用户、主机、授权集中由超级管理员配置。例如,必须由超级管理员(admin)新建用户、主机、授权,其他用户没有创建用户、主机、授权的权限。

12.3.2.2.1 新建用户

云盾堡垒机系统支持手工新建用户和批量导入用户两种添加方式。

12.3.2.2.1.1 手工新建用户

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到用户 > 用户管理页面,如图 12-28: 用户管理页面所示。

图 12-28: 用户管理页面

用户管	理		▶ 新建用户 更多操作 >
	删除 锁定 解锁	首页上一页	1/1 ~ 下一页 末页
Ċ	搜索用户名/姓名	Q	按角色过滤 ~
	用户		角色
	admin		超级管理员
			10 导出用户

- 3. 单击**新建用户**。
- 4. 在新建用户页面,输入用户信息,如图 12-29: 新建用户所示。

图 12-29: 新建用户

* 用户名	user01	最大长度16个字符
*角色	运维员 🔻	角色权限说明
* 密码	•••••	6-64个可见字符
	•••••	再次输入密码
* 姓名	张三	最大长度50个字符
邮箱	someone@example.com	最大长度100个字符
手机	138xxxxxxx	
备注		
创建用户		

单击角色选择框右侧的**角色权限说明**可查看云盾堡垒机系统所有角色的对应权限,如图 12-30: 角色权限说明所示。

图 12-30: 角色权限说明

	超级管理员	部门管理员	运维管理员	审计管理员	运维员	审计员	系统管理员
用 广管理 用户增加、删除、编辑	٠	٠	٠	٠			
用户组管理 用户组增加、删除、编辑	٠	٠	٠				
资产管理 管理资产	٠	٠	٠				
授 权管理 管理运维规则,审批工单	٠	٠	٠				
会话审计 查看、缅放、下载历史会话	٠	٠		٠		● 需要审计规则允许	
审计规则 管理审计规则	٠	٠		٠			
主机运维 主机运维、应用运维、创建工单、查看运维报表	٠	٠	٠	•	٠	٠	•
实时监控 管理、审批在线会话	٠	٠	٠				
系统管理 系统配置、操作日志、系统报表、数据维护、系统维护	•						•

5. 单击**创建用户**。

创建用户成功,系统提示用户已创建。

12.3.2.2.1.2 批量导入用户

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到用户 > 用户管理页面。
- 3. 单击更多操作,选择导入用户。
- 在导入用户页面,单击下载模板文件将用户列表模板下载至本地,如图 12-31: 导入用户页面所示。

图 12-31: 导入用户页面

导入用户
请上传由本系统导出的文件。或 下载模板文件 ,根据文件内提供的格式填写完成后上传到本系统。
上传文件
认证模式 本地认证 ▼
其他选项 🔲 覆盖已有同名用户
导入用户

5. 根据模板规范要求,制作需要导入的用户列表。

6. 单击上传文件,从本地选择制作好的用户列表文件。

7. 选择认证模式,勾选是否覆盖已有同名用户。



如不勾选覆盖已有同名用户,则同名用户不会被导入。

8. 单击**导入用户**。

等待用户导入完成,系统提示本次成功导入用户数量。

12.3.2.2.2 管理用户配置

背景信息

用户创建成功后,管理人员可以对用户进行相关配置。

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到**用户 > 用户管理**页面。
- 3. 单击已添加的用户,打开用户信息页面。
- 4. 选择用户配置页签,对该用户进行配置,单击保存更改,如图 12-32: 更改用户配置所示。

图 12-32: 更改用户配置



12.3.2.2.3 新建用户组

背景信息

用户组用于对用户进行分组或分类管理,一个用户可以属于多个用户组。

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到用户 > 用户组管理页面, 如图 12-33: 用户组管理页面所示。

图 12-33: 用户组管理页面

用	户纟	且管理	+ 新建用户组
[删除	
	С	授索用户组 Q	
		用户组名称	成员数

3. 单击**新建用户组**。

4. 填写用户组名称,单击创建用户组,如图 12-34:新建用户组所示。

图 12-34: 新建用户组

新建用户组

* 名称	user_group	最大长度50个字符
创建用户组		

用户组创建成功后,在**用户组管理**页面单击已添加的用户组,选择**修改用户组名称**页签,可修改 该用户组的名称。

12.3.2.2.4 对用户进行分组

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到**用户 > 用户组管理**页面。
- 3. 单击已添加的用户组,进入用户组信息页面。
- 4. 单击添加成员,在选择用户对话框中,勾选需要添加至该用户组的用户,单击添加,如图 12-35:
 选择用户所示。

在**选择用户**对话框中,可以输入用户名或姓名,单击查询按钮,只显示用户名/姓名包含所输入 字段的用户;也可以选择按角色进行过滤的方式,只显示属于某种角色的用户。

图 12-35: 选择用户

选择用	选择用户			
	添加	首页上一页	1/1 × 下一页 末页	
Ċ	搜索用户名/姓名	٥	按角色过滤 >	
	admin		超级管理员	
	user01 张三		运维员	
	user02 李四		审计管理员	
	user03 王五		系统管理员	

成功添加用户后,在**用户组信息**页面,勾选该用户组中的用户,单击**移除**,可将该用户从用户组 中移除。

12.3.2.2.5 新建主机

云盾堡垒机系统支持手工新建主机和批量导入主机两种添加方式。

12.3.2.2.5.1 手工新建主机

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到资产 > 主机管理页面, 如图 12-36: 主机管理页面所示。

图 12-36: 主机管理页面

主机	音理	+新建主机 导入主机
	删除 禁用 启用	首页 上一页 1/1 × 下一页 末页
Ċ	搜索主机名/主机IP Q	
	主机	主机帐户数
	主机 192.168.1.110 CentOS	主机帐户数 1
	<u>主机</u> 192.168.1.110 CentOS 192.168.1.120 web服务器	主机帐户数 1 1

3. 单击新建主机。

4. 在新建主机页面,输入主机IP、主机名称,如图 12-37:新建主机所示。

图 12-37: 新建主机

新建主机		
* 主机IP	192.168.1.100	支持IPv4地址和域名格式,例: 192.168.50.1 或者 www.example.com
主机名称	web服务器	最大长度50个字符
备注		
创建主机		



如果不填写主机名称,主机创建之后,默认使用主机IP作为主机名称。

5. 单击**创建主机**。

创建主机成功,系统提示主机已创建。

6. 在主机管理页面,单击已添加的主机IP,进入主机信息页面,如图 12-38: 主机信息页面所示。

图 12-38: 主机信息页面

基本信息	主机配置	主机帐户
主机信息		
主も	ЛIP*	192.168.1.110
主机	名称	CentOS
	备注	
	L	
保存更	改	



在基本信息页签中修改主机IP或主机名称,单击保存更改,可修改主机的基本信息。

7. 选择主机帐户页签,进入主机帐户管理页面,如图 12-39: 主机帐户管理所示。

图 12-39: 主机帐户管理

基本	真息 主机配置 主机帐户						
	□ 删除 添加主机帐户						
Ċ	捜索主机帐户 Q						
	主机帐户	协议	密码	SSH私钥	登录模式		
	无数据						

8. 单击添加主机帐户,打开新建主机帐户对话框,如图 12-40:新建主机帐户所示。

图 12-40: 新建主机帐户

新建主机帐户			×
		7	
协议	SSH		
登录模式	自动登录		
帐户类型	普通帐户		
主机帐户	user01		
	□ 特权帐户 □ 使用特权帐户改密	~	
密码	••••	验证	
	没有密码请留空		
创建主机帐户			

送 说明:

管理员可以创建一个**协议为SYSDEF、登录模式**为**手动的[EMPTY]**空帐户。SYSDEF协议表示可以手工选择任何协议方式登录主机。

运维人员使用[EMPTY]空帐户登录目标主机进行运维时,需要手动输入目标主机帐户和密码。

9. 配置主机帐户信息,单击验证,验证主机帐户和密码是否正确。

10.验证成功后,单击创建主机帐户。

后续操作

主机帐户创建成功后,在**主机管理**页面,可以查看已添加的主机及对应的主机帐户数。同时,在**主** 机帐户管理页面可管理已添加的主机帐号:

- 单击主机帐户名称,可在编辑主机帐户对话框中,修改该帐户的属性。
- 勾选主机帐户,单击删除,可删除主机帐户。
- 在已设置密码的主机帐户的密码栏中单击**清除**,可清除该主机帐户的密码。
- 对于使用SSH协议的主机帐户,如需通过SSH密钥方式登录,可在SSH私钥栏中单击**设置**来上传 对应的RSA私钥信息。

12.3.2.2.5.2 批量导入主机

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到资产 > 主机管理页面。
- 3. 单击**导入主机**。
- 在导入主机页面,单击下载模板文件将规范的主机列表模板下载至本地,如图 12-41:导入主机 页面所示。

图 12-41: 导入主机页面

导入主机
请上传由本系统导出的文件。或下载模板文件,根据文件内提供的格式填写完成后上传到本系统。
上传文件
其他选项 🔲 覆盖已有主机和主机帐户
导入主机

- 5. 根据模板规范,制作需要导入的主机列表文件。
- 6. 单击上传文件,从本地选择制作好的主机列表文件。
- 7. 勾选是否覆盖已有主机和主机帐户。



如不勾选覆盖已有主机和主机帐户,则同名主机和主机帐户不会被导入。

8. 单击**导入主机**。

等待主机和相应的主机帐户导入完成,系统提示本次成功导入数量。

12.3.2.2.6 管理主机配置

背景信息

主机添加成功后,管理人员可以对主机进行相关配置。

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到**资产 > 主机管理**页面。
- 3. 单击已添加的主机,打开**主机信息**页面。
- 4. 选择**主机配置**页签,对该主机进行配置,单击保存更改,如图 12-42:更改主机配置信息所示。

图 12-42: 更改主机配置信息

基本信息	主机配置 主机帐户
主机配置	
状态	□ 禁用这台主机
公子注闭	
2011/2010	
	◎ 丌但关时去问盖在
RDP选项	□ 启用键盘记录
	☑ 允许打印机/驱动器映射
	☑ 允许使用剪贴板下载
	☑ 允许使用剪贴板上传
SSH选项	☑ 允许X11转发
	☑ 允许隧道转发
	☑ 允许打开SFTP通道
	☑ 允许请求exec
文件传输	□ 生成文性SHΔ1
~11046	
伊方雨波	
TRAFFEER	

12.3.2.2.7 新建主机组

背景信息

主机组用于对主机进行分组或分类管理,一个主机可以属于多个主机组。

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到资产 > 主机组管理页面,如图 12-43: 主机组管理页面所示

图 12-43: 主机组管理页面

图 12-44: 新建主机组页面

主机约	且管理		+ 新建主机组
	删除		
Ċ	搜索主机组	٩	
	主机组名称		主机数
		无数据	

3. 单击新建主机组,进入新建主机组页面,如图 12-44:新建主机组页面所示。

新建主机组		
*	服友契约	最大长度50个字符
土竹城田有朴	NC 3-3 MARE	1807 KU200 5-13
创建主机组		

4. 填写**主机组名称**,单击**创建主机组**。

主机组创建成功后,在**主机组管理**页面单击已添加的主机组,选择**修改主机组名称**页签,可修改 该主机组的名称。

12.3.2.2.8 对主机进行分组

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到资产 > 主机组管理页面。
- 3. 单击已添加的主机组,进入主机组信息页面。
- 4. 单击添加主机,在选择主机对话框中,勾选需要添加至该主机组的主机,单击添加,如图 12-45:
 选择主机所示。

图 12-45: 选择主机

选择主	三村几					×
	添加	首页	上一页	1/1 ~	下一页	末页
Ċ	搜索主机名/主机IP					Q
	192.168.1.120 web服务器					



在**选择主机**对话框中,可以输入主机名或主机IP,单击查询按钮,只显示主机名/主机IP中包含 所输入字段的主机。

成功添加主机后,在**主机组信息**页面,勾选该主机组中的主机,单击**移除**,可将该主机从主机组 中移除。

12.3.2.2.9 运维授权

运维授权是为了梳理用户与主机之间的关系,本章节以基于用户授权主机账户的方式为例进行具体 说明。

12.3.2.2.9.1 新建运维规则

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到**授权 > 运维规则**页面。
- 3. 单击**新建运维规则**,进入**新建运维规则**页面,关联用户与资产的关系,如图 12-46: 新建运维规则页面所示。

图 12-46: 新建运维规则页面

* 规则名称		最大长度50个字符
规则有效期	-	不限制运维规则的有效期请留空
备注		
用户		资产
一删除	添加用户 ~	✓ 删除 添加资产 ∨
	请添加用户	请添加资产
创建运维规则		

- a) 填写规则名称,设置规则有效期。
- b) 单击**添加用户**, 选择**添加用户**或添加用户组。
- c) 勾选需要授权的用户或用户组,单击添加,如图 12-47: 添加用户页面所示。

图 12-47: 添加用户页面

添加用	户					×
	添加	首页	上一页	1/1	~ 下一页	末页
Ċ	搜索用户名/姓名			Q	按角色过滤	~
	admin				超级管理员	
	user01 张三				运维员	

- d) 返回新建运维规则页面,单击添加资产,选择添加主机帐户、添加帐户组或者添加主机组。
- e) 勾选需要授权的主机帐户、帐户组或者主机组,单击添加,如图 12-48: 添加主机帐户页面所

示。

图 12-48: 添加主机帐户页面

动中长	<u>ب</u>			×
	添加	首页 上一页	1/1	✓ 下一页 末页
C	搜索主机名/主机IP/主机帐户		Q	按协议过滤 ~
	192.168.1.120 web服务器	Administrator		RDP

4. 在新建运维规则页面,单击创建运维规则,即将所添加的用户和所添加的主机帐户进行关联。

12.3.2.2.9.2 管理运维规则

背景信息

运维规则创建后,管理人员可以对运维规则进行相关配置。

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到**授权 > 运维规则**页面。
- 3. 选择已添加的运维规则,执行相关操作。
 - 单击操作,选择编辑规则,可变更该规则的相关信息。
 - 在总览页签,可修改该规则的名称,设置有效期或直接禁用该规则。
 - 在用户/资产页签,可修改该规则中用户与主机之间的关系。
 - 在登录限制页签,可对该规则启用登录限制并进行相关设置,如图 12-49:设置登录限制所示。

图 12-49: 设置登录限制

总览 用户/资产	登录限制	命令控制	协议控制			
状态	□ 启用登录限制]				
来源IP限制模 式	(黑名单)不允;	F以下IP	V			
IP列表						
	4			۱.		
	填写点分十进制	洛式的IPv4地址	L或IP段,每行	只填写一个IP或	四 者一段IP,IP段的起	已始IP和结束IP之间用" - "
登录时段限制	0 1	2345	6789	10 11 12 13	14 15 16 17 18	19 20 21 22 23
	周二					
	周三					
	周五					
	周六					
	周日					
	🗌 允许	□ 禁止				
保存更改						

在命令控制页签,可对该规则启用命令控制并进行相关设置,如图 12-50:设置命令控制所示。

图 12-50: 设置命令控制

总范 用户/资产 登录限制 命令控制 协议控制		
状态 💷 屈用命令控制		
命令匹配优先说故:阻断会活 > 環要审范 > 周白名单 的顺序 描写命令以行力神位,每一行力一个命令神元(命令+参数),命 例:正配cortps命令,请该运cortp3时运动列表中,若要正配 例2:匹配ps命令及susort中任意一个参数;请该写ps *a**v* 5	岩行政穴匹配 ド和争取力規模匹配(文件通能行?*[]) にゅ行其近命令,遺領写on* *******19到血的列表中,身数匹配与顺序正关	
以下命令会阻断会话	以下命令需要审批	(黒名单)不允许执行以下命令 🔻
	4	
保行更改		

在协议控制页签,可对该规则启用协议控制并进行相关设置,如图 12-51:设置协议控制所示。

图 12-51: 设置协议控制

总览 用户/资产	登录限制 命令控制 协议控制
状态	■ 启用协议控制
会话选项	■ 开启会话二次审批
	□ 开启会话备注
	■ 开启历史会话审计
	☑ 开启实时会话监控
RDP选项	□ 启用键盘记录
	■ 允许打印机/驱动器映射
	■ 允许使用剪贴板下载
	■ 允许使用剪贴板上传
SSH选项	■ 允许X11转发
	■ 允许隧道转发
	■ 允许打开SFTP通道
	■ 允许请求exec
文件传输	□ 生成文件SHA1
	□ 保存文件
	☞ 保存下载文件
	☑ 保存上传文件
	□ 启用文件压缩
	☑ 不保存超过 30 KB 的文件
	☑ 单个会话保存的文件超过 100 MB 时停止保存

说明:

协议控制设置与主机配置内容相同,但协议控制启用后仅针对该运维规则授权的用户生效,而主机配置对所有用户生效。
- 单击操作,选择复制规则,在复制规则对话框中输入新规则的名称并选择复制内容,可复制 该规则的相关信息创建新的运维规则。
- 单击操作,选择删除规则,可删除该运维规则。

12.3.2.3 实时监控

背景信息

为运维人员配置运维规则后,运维人员就能通过云盾堡垒机系统对所授权的主机进行运维操作。在运维人员进行运维操作时,管理人员可以通过云盾堡垒机系统实时监控运维会话。

操作步骤

- 1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
- 2. 定位到**运维 > 实时监控**页面。
- 3. 选择所有会话页签,选择实时会话,执行更多操作。
 - 单击操作栏中的详情,可查看详细的会话信息。
 - 单击操作栏中的播放,可通过Web方式查看会话实时回放。

送 说明:

通过Web方式查看会话审计,需要在本地安装Flash Player才可在线播放。如果本地客户端 未安装Flash Player,单击云盾堡垒机系统页面右上角的用户名,选择**工具下载**,下载并安 装Flash Player 12。

• 单击阻断会话,可直接断开该实时运维会话,运维人员将被强制断开与目标主机的连接。

送 说明:

如果在运维规则中启用了命令控制功能,对于需要管理人员审批的命令,可在**实时监控**页面的需要审批命令页签查看详细信息,并进行审批操作。

12.3.3 运维人员操作指南

超级管理员参考快速配置手册为运维人员授权主机后,运维人员就能通过云盾堡垒机系统对所授权 的主机进行运维操作。云盾堡垒机系统支持运维人员通过Web运维方式和客户端运维方式两种方式 进行运维操作。

12.3.3.1 登录云盾堡垒机系统

前提条件

请确认您所使用的客户端能够正常访问云盾堡垒机系统。

操作步骤

- 1. 打开Chrome浏览器。
- 2. 在地址栏中,输入云盾堡垒机系统的访问地址,按回车键(Enter),进入系统登录页面。
- 3. 在云盾堡垒机系统登录页面,输入超级管理员所分配的用户名、密码,输入验证码。
- 4. 单击**登录**。

首次登录成功后,运维人员需要修改登录密码。

12.3.3.2 下载运维工具

背景信息

工具下载页面为运维人员提供在登录主机前下载所需要用到的运维工具。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 单击页面右上角的用户名,选择**工具下载**,进入**工具下载**页面,如图 *12-52:* 工具下载页面所示。

图 12-52: 工具下载页面

Т	工具下载						
	运维及ī	审计工具					
	名称		下载				
	6	单点登录器 运维登录必备工具	本地下载				
	ø	高线播放器 播放下载到本地的会话数据	本地下载				
	£	Adobe AIR 4.0 商线播放器运行环境	本地下载 MD5:66214913c51c9f7589e8fe3bcf66b05f				
	£	Flash Player 12 Flash播放器	本地下载 (IE浏览器版本) MD5:b165fd256a586cdcc2237b6f03e5a8bd 本地下载 (其他浏览器版本) MD5:16a84718fb300915e3c7ca7ea271eddc				
	浏览器						
	A						
	名称		下载				
	0	chrome 谷歌浏览器	本地下载 MD5:720ba977535b6ba24ce8b2524448ddb6				

3. 选择所需要的工具,单击**本地下载**,即可将相应的安装程序下载到本地进行安装。

表 12-1: 运维工具说明

运维工具	说明
单点登录器	单点登录器是通过Web方式调用客户端运维工具时,必须安装的登 录工具。
离线播放器	离线播放器与Adobe ATR是用于下载会话审计的会话日志后,进行
Adobe ATR	离线播放的工具。

运维工具	说明
Flash Player	Flash Player是通过Web方式查看会话审计的会话日志时,必须安装 的工具。
字符客户端	字符客户端包括PuTTY、SecureCRT、Xshell、Windows Telnet等 工具,用于连接SSH、Telnet协议的主机进行运维操作。
图形客户端	图形客户端包括Mstsc、RealVNC等工具,用于连接Windows服务 器、VNC服务器进行运维操作。
文件传输客户端	文件传输客户端包括FileZilla、WinSCP、SecureFX等工具,用于连 接SFTP、FTP服务器进行文件传输操作。

12.3.3.3 Web方式运维操作指南

本章节主要介绍通过云盾堡垒机系统的Web页面登录的方式对主机进行运维操作。

送 说明:

本章节中的操作步骤仅适用于使用Windows客户端的运维人员。

12.3.3.3.1 安装单点登录器

背景信息

单点登录器是Web方式运维必备工具。安装时,请注意不要被杀毒软件误拦截,建议关闭杀毒软件。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 单击页面右上角的用户名,选择工具下载,进入工具下载页面,如图 12-53: 工具下载所示。

图 12-53: 工具下载

🚢 user01 🔻	
Ⅲ 查看个人信息	
🕹 工具下载	
▶ 退出系统	

3. 定位到单点登录器,单击**本地下载**,将安装程序下载至本地客户端,如图 12-54:单点登录器下载所示。

图 12-54: 单点登录器下载

名称	下载
单点登录器 运维登录必备工具	本地下载

在本地客户端,双击单点登录器安装程序,选择语言,单击OK,单击安装。
 单点登录器安装完成后,提示安装成功,单击确定。

12.3.3.3.2 指定运维工具

背景信息

本章节以指定PuTTY工具为SSH协议登录方式为例介绍如何为SSH协议配置Web运维工具。您可以 参考本章节中的操作步骤为其它登录协议指定运维工具。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到运维 > 主机运维页面,单击右上角的Web运维配置。
- 3. 在Web运维配置对话框中,选择登录协议,例如选择SSH & TELNET & Rlogin。
- 4. 选择客户端程序,例如选择PuTTY。



确认您已安装了所选择的客户端程序。

5. 单击**保存**。

📃 说明 :

如果浏览器弹出**要打开**URL_:USM single-On**吗**_?的提示,单击**打开**URL:USM Single Sign-On。

6. 在单点登录配置对话框中,单击浏览,定位到所选择客户端程序所在的位置,单击打开,单击确定,如图 12-55:单点登录配置所示

图 12-55: 单点登录配置

单点登录配置		×
₽ ₿	单点登录配置	
选择客户端 PuTTY >	C:\Program Files (x86)\putty_V0.63.0.0.43510830.exe	浏览
	确定	取消

配置成功后,弹出提示对话框,如图 12-56:单点登录配置成功所示。

图 12-56: 单点登录配置成功



12.3.3.3.3 主机运维

12.3.3.3.3.1 通过SSH协议登录主机进行运维

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到运维 > 主机运维页面。

说明:
在搜索框中输入主机IP、主机名、帐户等关键字信息,系统会自动过滤相关的目标主机。
3. 选择已授权的SSH协议的主机帐户,单击登录,如图 12-57: SSH协议主机Web运维所示。



如果浏览器弹出**要打开**URL_:USM single-On吗_?的提示,单击**打开**URL:USM Single Sign-On。

图 12-57: SSH协议主机Web运维

主机运维	快速运维:输入主机名/	主机IP/帐户			✿ Web运维配置
按运维规则过滤	~			首页 上─页 1/1 ×	下一页末页
搜索主机名/主机	Up Q	按主机组过滤 ~			
主机		主机组	主机帐户		登录
192.168.1.110 (CentOS		[SSH] root	T	登录 ●〕
192.168.1.120	windows	业务服务器	[RDP] Administrator	Ŧ	登录 ●〕

- 4. 自动启动SSH运维工具,即可登录到目标主机中进行运维操作,如图 12-58: SSH协议主机运维操作所示。
 - 图 12-58: SSH协议主机运维操作





如果使用[EMPTY]空帐户登录目标主机,需要手动选择协议,并输入目标主机帐户和密码。

12.3.3.3.3.2 通过RDP协议登录主机进行运维

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到**运维 > 主机运维**页面。



在搜索框中输入主机IP、主机名、帐户等关键字信息,系统会自动过滤相关的目标主机。

3. 选择已授权的RDP协议的主机帐户,单击登录,如图 12-59: RDP协议主机Web运维所示。



如果浏览器弹出**要打开**URL_:USM Single-On**吗**_?的提示,单击**打开**URL:USM Single Sign-On。

图 12-59: RDP协议主机Web运维

主机运维 快速运维:输入主机名/		主机IP/帐户			✿ Web运维配置
按运维规则过滤	~		首页上一	页 1/1~	下一页末页
搜索主机名/主机	LIP Q	按主机组过滤 ~			
主机		主机组	主机帐户		登录
192.168.1.110	CentOS		[SSH] root	T	登录 €
192.168.1.120 v	windows	业务服务器	[RDP] Administrator	Ŧ	登录 ●〕

- 4. 单击确定,启动远程桌面连接工具。
- 5. 在远程桌面连接对话框中,单击连接,即可登录到目标主机中进行运维操作,如图 12-60: RDP协议主机运维操作所示。

图 12-60: RDP协议主机运维操作

Ng产IP) - USM - 10.000 - 10.000 - 10.000 - 5.000 - 5.0000 - 5.00000 - 5.0000000000	夏面连接			-	· .) ×
Registe Bri						
witz:	Printial Configuration Tasks	is server	EICI2			
	Provide Computer Information		Specifying computer information			
EmEditor	🐴 Activate Windows	Product ID:	55041-507-1099763-84081 (Activated)			
	eff Set time gone	Time Zone:	(UTC+08.00) Beijing, Chongqing, Hong Kong, Ukunqi			
mo 6.9.2 bin	Service Detworking	Local Area Connection	s 192.168.50.194, IPv6 enabled			
	😹 Provide computer name and domain	Full Computer Name: Workgroup:	WIN-78UTEOGK40V WORKGROUP			
	② Update This Server		Updating your Windows server			
emad64_16	🍇 Enable automatic updating and feedback	Updates: Feedback:	Not configured Windows Encr Reporting off Not participaling in Customer Experience Improvement Program			
Subine Test	Ownload and install updates	Checked for Updates: Installed Updates:	Nevel Nevel			
	Customize This Server		Customizing your server			
	🙀 Add roles	Roles:	Remote Desktop Services			
ττ ι	Add (eatures	Features:	Remote Server Administration Tools			
	🔩 Enable Remote Des <u>k</u> top	Remote Desktop:	Enabled			
	Configure Windows Firewall	Firewall:	Private: On			
	Print, e-mail, or gave this information					
	Do not show this window at logon		Dose			
<						,



如果使用[EMPTY]空帐户登录目标主机,需要手动选择协议,并输入目标主机帐户和密码。

12.3.3.3.3.3 通过SFTP协议登录主机进行运维

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到运维 > 主机运维页面。



在搜索框中输入主机IP、主机名、帐户等关键字信息,系统会自动过滤相关的目标主机。

3. 选择已授权的SFTP协议的主机帐户,单击登录,如图 12-61: SFTP协议主机Web运维所示。

送 说明:

如果浏览器弹出**要打开**URL_:USM single-On**吗**_?的提示,单击**打开**URL:USM Single Sign-On。

图 12-61: SFTP协议主机Web运维

主机运维 快速运维:输入主机名/主机IP/帐户			✿ Web运维配置
按运维规则过滤		首页 上─页 1/1 ~	下一页末页
搜索主机名/主机IP Q	按主机组过滤 ~		
主机	主机组	主机帐户	登录
192.168.1.110 CentOS		[SFTP] root	登录 🔊
192.168.1.120 windows	业务服务器	[RDP] Administrator	登录 🔊
192.168.1.125 Windows服务器		[RDP] Administrator	登录 €

4. 自动启动SFTP运维工具,即可启动客户端工具连接到目标主机进行运维操作,如图 12-62: SFTP协议主机运维操作所示。

图 12-62: SFTP协议主机运维操作

🌯 Documents - admin@10.11.1.2 - WinSCP – 🗆 🗙								
本地(L)标记(M)文件(F)命令	ݤ(C) 会话(S) រ	选项(O) 远程(F	R) 帮助(H)					
🔹 💷 🗸 - 🟦 😫 🐼 🔤 📓								
📲我的文档 🔹 🔄	(🗴 🖄 🖄 皆] root	- 🔄 4		🔁 🚮 🔯 📴		
C:\Users\ding_c\Documents			/root	-				
名字扩展大小	类型	已改变 ^	名字扩展	大小	已改变	权限 ^		
⁼	上级目录	2016/1	<u>⊾</u>		2016/11/2	r-xr-xr-x		
AIDA64 Reports	文件夹	2016/8	.cache		2016/11/1	rwx		
Fiddler2	文件夹	2016/9	.gnupg		2016/11/1	rwx		
Integration Ser	文件夹	2016/8	📕 .pki		2016/11/1	rwxr		
Integration Ser	文件夹	2016/8	.ssh		2016/11/1	rwx		
My Knowledge	文件夹	2016/9	📜 .vnc		2016/11/2	rwxr-xr->		
🐌 My Music	文件夹	2016/9	.bash_history	8,941	2016/12/2	rw		
🔚 My Pictures	文件夹	2016/9	🗋 .bash_logout	18	2009/5/20	rw-rr		
🖪 My Videos	文件夹	2016/9	🗋 .bash_profile	176	2009/5/20	rw-rr		
📜 NetSarang	文件夹	2016/7	.bashrc	176	2004/9/23	rw-rr		
📙 QQPCMgr	文件夹	2016/9	.cshrc	100	2004/9/23	rw-rr		
📜 SQL Server Ma	文件夹	2016/1	.tcshrc	129	2004/12/4	rw-rr		
Tencent Files	文件夹	2016/1	.viminfo	5,359	2016/11/3	rw		
📕 Virtual Machines	文件夹	2016/1	🗋 .Xauthority	66	2016/11/2	rw		
 Visual Studio 2 	かけま	2016/0	Canaconda-ke cfr	A 867	2012/12/5	>		
0 B of 73,203 KiB in 0 of 37			0 B of 267 MiB in 0 of 18					
✔ F2 重命名 F4 编辑 F5	🔐 F2 重命名 📝 F4 编辑 🖻 F5 复制 ^屆 F6 移动 誉 F7 创建目录 🗙 F8 删除 💣 F9 属性 🗓 F10 退出							
				۵	SFTP-3	0:04:00		
0								
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □								

如果使用[EMPTY]空帐户登录目标主机,需要手动选择协议,并输入目标主机帐户和密码。

12.3.3.3.3.4 未授权登录主机进行运维

背景信息

如果运维人员知道某主机的IP、账户和密码信息,但该主机未被授权,不在主机运维列表中显示。 此时,运维人员可以通过未授权登录的方式登录该主机进行运维操作。

| ■ 说明:

未授权登录功能默认禁用,需要超级管理员或系统管理员在**系统 > 系统设置**页面中启用该功能后 才可以使用。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到运维 > 主机运维页面,单击未授权登录,如图 12-63:未授权登录所示。

主机运维 ➡ 未授权登录 ✿ Web运维配置 快速运维:输入主机名/主机IP/帐户 按运维规则过滤 \sim 首页 上一页 1/1 ~ 下一页 末页 搜索主机名/主机IP Q 按主机组过滤 \checkmark 主机组 主机帐户 登录 主机 [SSH] root 登录 ●〕 192.168.1.110 CentOS Ŧ 192.168.1.120 windows 业务服务器 [RDP] Administrator v 登录 ●〕 192.168.1.125 Windows服务器 登录 ●) [RDP] Administrator ۳

3. 在运维登录对话框中,输入主机IP等信息,单击确定,即可登录目标主机,如图 12-64: 未授权 运维登录对话框所示。

图 12-63: 未授权登录

图 12-64: 未授权运维登录对话框

运维登录		×
主机IP*	192.168.1.115	
协议	SSH 🔹]
端口	22	
帐户名称	root]
密码	•••••	
确定取消		

通过未授权登录方式登录主机后,管理人员可在**授权 > 未授权登录审核**页面查看相关登录记 录。

12.3.3.3.3.5 运维审批申请

背景信息

对于在主机配置中启用开启会话二次审批功能的主机,即使运维人员在主机运维页面可以看到该主

机,也无法直接登录。运维人员单击登录后,系统会自动生成运维申请,需要由管理人员审批通过

后,运维人员才能登录主机进行运维操作。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到运维 > 运维审批页面,查看系统已自动生成的运维审批申请记录及审批状态。

对于已被批准的运维申请,运维人员即可在**主机运维**页面通过Web方式登录该主机进行运维操 作,且该运维申请的状态将变为已登录。

12.3.3.4 CS方式运维操作指南

除上一章节中介绍的通过Web方式进行运维操作外,云盾堡垒机系统也支持通过客户端方式进行运维操作。

本章节主要介绍运维人员通过客户端登录云盾堡垒机系统,再访问目标主机的运维方式。

12.3.3.4.1 苹果系统客户端运维操作指南

12.3.3.4.1.1 准备工作

在使用苹果系统客户端登录云盾堡垒机系统进行主机运维操作前,请确保已完成下列准备工作:

- 本地已安装支持SSH协议的app,例如命令行终端、SecureCRT、Xshell等。
- 本地已安装支持RDP协议的app,例如远程桌面连接。
- 确保苹果系统客户端与云盾堡垒机系统的端口正常连通,主要包括以下两个端口:
 - 60022:用于访问SSH协议的主机。
 - 63389:用于访问RDP协议的主机。
- 确保云盾堡垒机系统与目标主机的运维端口正常连通,例如SSH协议及端口、RDP协议及端口。

12.3.3.4.1.2 通过命令行终端app的菜单方式登录目标主机进行运维

背景信息

本章节以命令行终端app为例,通过SSH协议登录目标主机进行运维。您可以参考本章节中的操作 步骤使用其它app登录SSH协议的主机帐户。

操作步骤

1. 打开命令行终端app,输入以下命令,按回车键(Enter),如图 12-65:通过命令行终端登录云 盾堡垒机所示。

ssh 云盾堡垒机系统的用户名@云盾堡垒机系统的IP -p60022



如果提示需要输入密码,请输入该用户的密码,按回车键(Enter)。

- 云盾堡垒机系统的用户名指代管理员(例如admin)所创建的用户名。
- 云盾堡垒机系统的IP指代云盾堡垒机系统的IP地址,请根据实际情况输入。

图 12-65: 通过命令行终端登录云盾堡垒机

2. 进入资产管理界面,通过上下键选择已授权的主机资产,按回车键(Enter),如图 12-66: 通过 命令行终端选择主机资产所示。

图 12-66: 通过命令行终端选择主机资产

	😭 iben — USN	IShell — ssh — 80×24	
1 10.1.2.33 2 192.168.21.168 3 192.168.27.49 4 192.168.27.84 5 192.168.50.112 6 192.168.50.113 7 192.168.50.114 8 192.168.50.115	 10.1.2.33 192.168.21.168 windows2008 llinux 主机名称 主机名称 主机名称 主机名称 主机名称 主机名称 	<pre>(1:test) (1:[EMPTY]) (1:administrator) (2) (1:[EMPTY]) (1:[EMPTY]) (1:[EMPTY])</pre>	8
Type ":h <enter>" for</enter>	basics learning.	4,8 50%	_ [

3. 选择主机账户,按回车键(Enter),如图 12-67: 通过命令行终端选择主机帐户所示。



如提示需要输入密码,请输入该主机帐户的密码,按回车键(Enter)。

图 12-67: 通过命令行终端选择主机帐户



登录目标主机进行运维操作,如图 12-68: 通过命令行终端登录目标主机所示。

图 12-68: 通过命令行终端登录目标主机

12.3.3.4.1.3 通过远程桌面连接app的菜单方式登录目标主机进行运 维

背景信息

本章节以远程桌面连接app为例,通过RDP协议登录目标主机进行运维。您可以参考本章节中的操 作步骤使用其它app登录RDP协议的主机帐户。

操作步骤

1. 打开远程桌面连接app,输入<云盾堡垒机系统IP>:63389,单击连接,如图 12-69:通过远程桌面连接登录云盾堡垒机系统所示。



其中,<云盾堡垒机系统的IP>指代云盾堡垒机系统的IP地址,请根据实际情况输入。

图 12-69: 通过远程桌面连接登录云盾堡垒机系统

	远程桌面连接	
×	™™™ 适用于 Mac 的远程桌面连接	
计	算机: 192.168.27.71:63389 (示例: MyPC, name.microsoft.com, 192.168.2.8)	连接

2. 在**是否仍要连接此计算机**?对话框中,单击**连接**,如图 *12-70:*通过远程桌面连接连接云盾堡垒 机系统所示。

图 12-70: 通过远程桌面连接连接云盾堡垒机系统

00			
M		证书上的服务器名称不正确。 是否仍要连接到此计算机?	
	<u> </u>	取消 连接	

- 3. 在云盾堡垒机系统登录窗口,输入云盾堡垒机系统的用户名和密码,单击**登录**,如图 12-71:登录云盾堡垒机系统所示。
 - 369

 用户名:

 admin

 369:

 1

 358

 現出
 - 图 12-71: 登录云盾堡垒机系统

4. 在资产管理界面,双击选择已授权的主机资产,或者通过搜索框搜索主机资产,如图 *12-72*:通过远程桌面连接选择主机资产所示。



如提示需要输入密码,请输入该主机帐户的密码,单击登录键。

图 12-72: 通过远程桌面连接选择主机资产

授权主机 未授权登陆	192			
主机名	IP	账户名	端口	
windows2008	192.168.27.49	administrator	3389	
windows2008	192.168.27.49	user	3389	
2003	192.168.27.47	administrator	3389	
10.1.2.33	10.1.2.33	administrator	3389	
			1	主销

登录目标主机进行运维操作,如图 12-73: 通过远程桌面连接登录目标主机所示。



图 12-73: 通过远程桌面连接登录目标主机

12.3.3.4.2 Windows系统客户端运维操作指南

12.3.3.4.2.1 准备工作

在使用Windows系统客户端登录云盾堡垒机系统进行主机运维操作前,请确保已完成下列准备工 作:

- 本地已安装支持SSH协议的运维工具,例如PuTTY、SecureCRT、Xshell等工具。
- 本地已安装支持RDP协议的运维工具,例如Windows系统自带的远程桌面连接工具。
- 本地已安装支持SFTP协议的运维工具,例如WinSCP、XFTP、FlashFXP等工具。
- 本地已安装支持FTP协议的运维工具,例如XFTP、FlashFXP等工具。
- 确保Windows系统客户端与云盾堡垒机系统的端口正常连通,主要包括以下端口:
 - 60022:用于访问SSH、Telnet、SFTP协议的主机。
 - 63389:用于访问RDP协议的主机。
 - 60021:用于访问FTP协议的主机。
- 确保云盾堡垒机系统与目标主机的运维端口正常连通,例如SSH协议及端口、RDP协议及端口。

📕 说明 :

SFTP、FTP协议的主机账号和密码必须设置为自动登录。通过客户端方式进行SFTP、FTP协议主机运维时,主机帐号和密码必须已在云盾堡垒机系统中配置,不支持手动登录。

12.3.3.4.2.2 通过SSH工具登录目标主机进行运维

背景信息

本章节以PuTTY工具为例,通过SSH协议登录目标主机进行运维。您可以参考本章节中的操作步骤 使用其它运维工具登录SSH、Telnet协议的主机帐户。

操作步骤

1. 打开PuTTY工具,在登录窗口中输入云盾堡垒机系统的IP和端口号(60022),单击Open,如图 *12-74*: 连接云盾堡垒机所示。

图 12-74: 连接云盾堡垒机

🕵 PuTTY Configuration	
Putty Configuration Category: Session Logging Terminal Keyboard Bell Features Window Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 10. 131 60022 Connection type: Raw Telnet Rlogin SSH Serial Load, save or delete a stored session Saved Sessions Default Settings Load Save Delete
About	Close window on exit: Always Never Only on clean exit Open Cancel

2. 输入云盾堡垒机系统的用户名和密码,按回车键(Enter),如图 12-75: 登录云盾堡垒机所示。

图 12-75: 登录云盾堡垒机



3. 进入资产管理界面,通过上下键选择已授权的主机资产,按回车键(Enter),如图 *12-76*:选择 主机资产所示。

图 12-76: 选择主机资产

🖉 USMShell			
" Quit: Use " Move: Use " Search: Use " Jump: Use " Command: Use " Use " Refresh: Use " Language: Use	<pre>":q<enter>". the cursor keys, or "/{patten}<enter>" a ":{number}<enter>" t ":[ssh telnet rlogin ":[ping traceroute c "r" to refresh lists "e" to change langua</enter></enter></enter></pre>	"j" to go nd then "n o jump to] [-1 use: onnect] {} ge encodir	<pre>down, "k" to go up, "u" to PageUp n"/"N" to next/privous searching r line {number}. r] {user}@{host}:{port} [-p port]< host} [port]<enter>" for check ng between UTF-8 and GB2312.</enter></pre>
[usmshell] 001: CentOS 002: CentOS 003: openSUSE	192.168.1.110:22 192.168.1.110:0 192.168.1.115:22	ssh sysdef ssh	root [EMPTY] root

- 4. 在USERNAME中输入主机帐户,按回车键(Enter),如图 12-77: 输入主机帐户所示。
 - 图 12-77: 输入主机帐户

🕼 USMShell 💼 📼 📼	X
<pre>" Quit: Use ":q<enter>". " Move: Use the cursor keys, or "j" to go down, "k" to go up, "u" to PageUp " Search: Use "/{patten}<enter>" and then "n"/"N" to next/privous searching r " Jump: Use ":{number}<enter>" to jump to line {number}. " Command: Use ":[ssh telnet rlogin] [-1 user] {user}@{host}:{port} [-p port]< " Use ":[ping traceroute connect] {host} [port]<enter>" for check " Refresh: Use "r" to refresh lists. " Language: Use "e" to change language encoding between UTF-8 and GB2312.</enter></enter></enter></enter></pre>	*
[usmshell]	ш
	•

5. 在PROTOCOL中,输入ssh,按回车键(Enter),如图 12-78:输入SSH协议所示。

图 12-78: 输入SSH协议

B USMShell	٢.
<pre>"</pre>	*
[usmshell]<< PROTOCOL >> 001: CentOS 192.168. ssh 002: CentOS 192.168press CTRL-C close] 003: openSUSE 192.168.1.115:22 ssh root	
	4 M

6. 在主机登录界面,输入主机帐户的密码,按回车键(Enter),如图 *12-79*: 输入主机帐户密码所示。

图 12-79: 输入主机帐户密码



登录目标主机进行运维操作,如图 12-80: 通过PuTTY工具登录目标主机所示。

图 12-80: 通过PuTTY工具登录目标主机

🛃 root@ 🔤 🔤 🗾 🖂	
Permission denied, please try again.	•
(usmshell) rootg1.110:22-CentOS's password: Last login: Thu Apr 19 17:45:39 2018 from 192.168.1.2	
Welcome to Alibaba Cloud Elastic Compute Service !	
[root@i .Z ~]#	
	=
	Ŧ

12.3.3.4.2.3 通过远程桌面连接工具的菜单方式登录目标主机进行运 维

背景信息

本章节以远程桌面连接(MSTSC)工具为例,通过RDP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录RDP协议的主机帐户。

操作步骤

1. 打开远程桌面连接工具,输入<云盾堡垒机系统IP>:63389,单击连接,如图 12-81:通过远程 桌面连接工具登录云盾堡垒机系统所示。



其中,<云盾堡垒机系统IP>指代云盾堡垒机系统的IP地址,请根据实际情况输入。

图 12-81: 通过远程桌面连接工具登录云盾堡垒机系统

😼 远程桌面递	接		
	远程桌面 连接		
计算机 (C):	192. 168. 27. 71 : 63389	•	•
用户名:	WIN-N3TPNPA05J7\user		
当您连接时料	将向您询问凭据。		
😠 选项 @)	I		帮助创

2. 在是否信任此远程连接?对话框中,单击连接,如图 12-82:通过远程桌面连接工具连接云盾堡 垒机系统所示。

图 12-82: 通过远程桌面连接工具连接云盾堡垒机系统

150 远程桌	面连接	×
ぞ 是	否信任此远程连接?	
此远程道	接会损坏您的本地或	远程计算机。请确保您在连接之前信任此远程计算机。
N	类型: 远程计算机:	远程桌面连接 192. 168. 27. 71
🔲 不再说	间问我是否连接到此讨	算机 @)
💽 详细	信息 @)	

- **3.** 在**无法验证次远程计算机的身份。是否仍要连接**?对话框中,单击**是**,如图 *12-83*: 通过远程桌面连接工具连接云盾堡垒机系统所示。
 - 图 12-83: 通过远程桌面连接工具连接云盾堡垒机系统

▶ 远程桌面连接
① 无法验证此远程计算机的身份。是否仍要连接?
由于安全证书存在问题,因此远程计算机无法通过身份验证。继续操 作可能不安全。
名称不匹配
□▲ 请求的远程计算机: 192.168.27.71
□ 来自远程计算机的证书中的名称: BAOLEIJI
证书错误
验证远程计算机的证书时遇到下列错误:
🤼 证书上的服务器名错误。
🚹 证书来自不信任的证书验证机构。
您想连接到远程桌面而忽略这些证书错误吗?
🔲 不再询问我是否连接到此计算机 (0)
査看证书(V) 是(X) 否(X)

- 在云盾堡垒机系统登录窗口,输入云盾堡垒机系统的用户名和密码,单击登录,如图 12-84:登 录云盾堡垒机系统所示。
 - 图 12-84: 登录云盾堡垒机系统



5. 在资产管理界面,双击选择已授权的主机资产,或者通过搜索框搜索主机资产,如图 12-85:通过远程桌面连接选择主机资产所示。



如提示需要输入主机用户名和密码,请输入该主机的用户名和密码,单击登录键。

图 12-85: 通过远程桌面连接选择主机资产

登录目标主机进行运维操作,如图 12-86: 通过远程桌面连接登录目标主机所示。

图 12-86: 通过远程桌面连接登录目标主机

5 192.168.27.71	-63389 - 远程桌面连接	TAXABLE PARTY AND AND ADDRESS OF TAXABLE PARTY.	
	uty		<u>م</u>
Wiware vSph	twist in the second sec		
Dasusmvi Si	ng)14		
PLSQL lice Developer	nse (P
iexplore 3	5093		
NetApp DnComman	\$222		
11907			

12.3.3.4.2.4 通过WinSCP工具登录目标主机进行运维

背景信息

本章节以WinSCP工具为例,通过SFTP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录SFTP协议的主机帐户。

📕 说明:

SFTP协议的主机账号和密码必须设置为自动登录。

操作步骤

1. 打开WinSCP工具,在登录窗口中输入云盾堡垒机系统的IP、端口号(60022)、用户名、密码,单击登录,如图 12-87:通过WinSCP工具登录云盾堡垒机系统所示。

图 12-87: 通过WinSCP工具登录云盾堡垒机系统

WinSCP 登录			? ×
会话 存储的会话 日志 环境 目录 SFTP SFTP SCP/Shell 连接	会话 主机名(山) 192.168.27.70 用户名(山) admin 密钥文件(L)	密码(P)	端口号(R) 60022 ★
○174里 一隧道 SSH 一密钥交换 一验证 一漏洞检测	 协议 文件协议ED	SFTP 🔻 🗹 允许	GCP反馈(E)
选项 			选择颜色②
关于® La	anguages	登录 保存	×(S) 关闭

2. 在右侧的主机列表中,双击已授权的主机资产,进入该主机的文件目录,如图 12-88:通过WinSCP工具选择主机资产所示。

图 12-88: 通过WinSCP工具选择主机资产

🌆 / - admin@192.168.27.	70 - WinSCP							
本地(L) 标记(M) 文件(F) 命令(C) 会话(S) 选项(Q) 远程(R) 帮助(H)								
🌔 🗏 🗊 • 🟦 😫	📀 🔤 🧬 😤 🐘	-	▼ ♀ ∅ ◯ 默认 - ◎ ダ -					
📔 我的文档 🔻 🔄 🗇	🖻 🔯 🙆	te	📔 / <root> 🔹 🔄 🕁 🔹 🔝 🖆 🛃 🚱</root>					
C:\Users\Administrator\Docum	ents		1					
名字扩展	大小 类型	*	名字 扩展 ^					
퉬 Axure	文件夹		H4-root@192.168.27.83:22					
🐌 Downloads	文件夹							
퉬 ihelper	文件夹							
🐌 Inpor	文件夹	=						
🜗 My Music	文件夹							
🖹 My Pictures	文件夹							
📄 My Videos	文件夹							
NetSarang	文件夹							
퉬 teiron	文件夹							
🐌 Tencent Files	文件夹							
1 我的显图	→仕車	Ŧ						
	U B of 2,/34 B in U of 16 0 B of 0 B in 1 of 1							
■ # F2 里萨洛 II F4 编辑	□圖 F3 复制 □圖 F0 移动 🎬	F/ 8	加建日來 ∧ ٢δ 删除 ٢9 唐注 』, FIU 返出					
			🔒 SFTP-3 🗐 0:00:29					

登录目标主机进行文件传输操作,如图 12-89: 通过WinSCP工具操作目标主机所示。

图 12-89: 通过WinSCP工具操作目标主机

🌆 root - admin@192.168.27.70 - Wi	inSCP									
本地(L)标记(M)文件(F)命令(C)	会话(<u>S</u>) 选项(<u>O</u>) 远程	(民) 帮助(日)								
🔹 🐵 🖓 🔹 🔐 🔐 🖉	P 😤 🗛 主 🖃	▼ 2 0 野认 - 頌 -								
▶ 我的文档 🔹 🔄 🖓 🗸 🕁 🔹	🖻 🔯 🚮 🙋 皆	📔 root 🔹 🗸 🗢 🔹 🔝 📶 🛃								
C:\Users\Administrator\Documents		/root								
名字 扩展 大小	▲ 类型 ▲	名字 扩展	-							
\mu Axure	文件夹	3 .								
\mu Downloads	文件夹	June								
퉬 ihelper	文件夹	\mu .gconfd	=							
🐌 Inpor	文件夹	遇 .ssh								
🚺 My Music	文件夹	.bash_history								
🖹 My Pictures	文件夹	.bash_logout								
📑 My Videos	文件夹	bash_profile								
🐌 NetSarang	文件夹	bashrc								
\mu teiron	文件夹	.cshrc								
🐌 Tencent Files	文件夹	tcshrc								
1. 我的母母	→仕中	Xauthority	-							
0 B of 2 734 B in 0 of 16 0 B of 40 781 B in 0 of 15										
IP F2 重命名 IP F4 编辑 1 F5 复新	비 🗳 F6 移动 💣 F7 f	測建目录 🗙 F8 删除 💣 F9 属性 <u>県</u> F10 退出								

12.3.3.4.2.5 通过XFTP工具登录目标主机进行运维

背景信息

本章节以XFTP工具为例,通过FTP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录FTP协议的主机帐户。

☐ 说明:

FTP协议的主机账号和密码必须设置为自动登录。

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 在页面右上角,单击用户名,选择查看个人信息,如图 12-90: 查看个人信息所示。

图 12-90: 查看个人信息



3. 在个人信息页面,选择cs登录口令页签,设置一个CS登录口令,单击保存更改,如图 12-91:设置CS登录口令所示。

送明:	
CS登录口令用于以FTP客户端登录系统	•

图 12-91: 设置CS登录口令

个人信息						
个人信息	修改密码	SSH公钥	SSH私钥	CS登录口令	手机身份验证	器
CS登录口令	用于以FTP客户	端登录系统				
CS登封	录口令				显示密码 6-	64个可见字符
保存更改						

4. 打开XFTP工具,在登录窗口中输入云盾堡垒机系统的IP、端口号(60021)、用户名、CS登录口令,选择FTP协议,单击确定,如图 12-92:通过XFTP工具登录云盾堡垒机所示。

说明	:	

此处的密码需填写在上述步骤中设置的CS登录口令。

图 12-92: 通过XFTP工具登录云盾堡垒机

<i>9</i> 桌	面 - Xftp 5				
Ŷ	新建会话属性		? <mark>×</mark>		
	常规 选项				-
	_FTP 站点			▼ 用尸名	名消
•	名称 (2):	堡垒机			
-	主机 (H):	192. 168. 27. 70			- 🖬 C-
名称	协议(图):	FTP	▼ 设置(S)		
i 🖳 t	端口号 @):	60021 🚔			
	代理服务器(2):	(元)	▼ 浏览 @)		
	说明 @):				
B 4					
<u></u> e					
	■ 匿名登录 (A)				
	□ 使用身份验证(代理 (G)			
1	方法(M):	Password	▼ 设置(S)		
)	用户名 (1):	admin			-
传辅	密码(E):	•••••			
名称	用戶密钥低:		▼ _ 浏览 @)	本地路径	<-> 远程器
	密码 ビバ				
•			确定 取消		+
就绪				116 对象	157.38MB

5. 在右侧的主机列表中,双击已授权的主机资产,进入该主机的文件目录,如图 12-93:通过*XFTP*工具选择主机资产所示。

图 12-93: 通过XFTP工具选择主机资产

🛷 网络 - Xftp 5					
文件(E) 编辑(E) 查看	(V) 命令(C) 工具((T) 窗口(W) 帮	助(<u>H</u>)		
🗖 🖬 • 🛛 🖉 🖉 🗌	🐺 🖻 🛛 🗎 🖬	🔁 🗋 🗗	s 🕫 🔅 🕐	P	-
☐ 主机名或IP地址			-	用户名	密码
● 网络 ×		${} $	● 堡垒机 ×		
🗲 🔿 📬 网络		- 🖬 O	← → 强 /		- 🖬 O
名称	大小 类型	修改时间	名称	^	
🍑	文件夹	E	퉬 H6-ftp@192.16	8.28.241:21	
	1	•	(III		4
传输日志					
名称	状态	进度	大小	本地路径	<-> 远程路
<	III			0.215	6 Potes
机结			进制	0 刈漏	0 Bytes

登录目标主机进行文件传输操作,如图 12-94: 通过XFTP工具操作目标主机所示。

图 12-94: 通过XFTP工具操作目标主机

💋 堡垒机 - Xftp 5					
文件(F) 编辑(E) 查看	請(V) 命令(C) 工具(T) 窗口(W) 帮!	助(H)		
📑 🖬 🖬 🖌 💉 🖉	🙀 Þ • 🖨 🗟	🔿 🛈 🖻	s 🕫 🗘 📀	P	
🗄 主机名或IP地址			-	用户名	密码
● 网络 ×		\rightarrow	● 堡垒机 ×		
🗲 🔿 📬 网络		- 🖬 C-	🗲 🔿 퉬 /新建	文件夹/	- 🖬 C
名称	大小 类型	修改时间	名称	<u>^</u>	
· 🛺	文件夹				
1			New File		
۰ III III III III III III III III III I	11	•	٠ III		,
传输 日志					
名称	状态	进度	大小	本地路径	<-> 远程
•	m				•
已连接 192.168.27.70:60021,	•		二进制	1 对象	0 Bytes

12.3.4 审计管理员操作指南

12.3.4.1 登录云盾堡垒机系统

前提条件

请确认您所使用的客户端能够正常访问云盾堡垒机系统。

操作步骤

- 1. 打开Chrome浏览器。
- 2. 在地址栏中,输入云盾堡垒机系统的访问地址,按回车键(Enter),进入系统登录页面。
- 3. 在云盾堡垒机系统登录页面, 输入审计管理员用户名、密码及验证码。



审计管理员的用户名及密码是由超级管理员所创建的。

4. 单击**登录**。

首次登录成功后,审计管理员需要修改密码。

12.3.4.2 审计

审计功能用于审计管理员对主机的访问操作的日志进行审计。

12.3.4.2.1 会话审计

会话审计页面用于记录运维人员对主机操作过程的会话日志。

12.3.4.2.1.1 查看所有会话

操作步骤

- 1. 登录云盾堡垒机系统。
- 定位到审计 > 会话审计 > 页面,选择所有会话,查看字符、图形、文件、应用类型的会话审计日志,如图 12-95: 查看所有会话所示。

图 12-95: 查看所有会话

会话审试	<i>.</i> †						
所有会话	音 事件查询						
ŧ	か议 全部 <u>捜索</u>	~ 展开更多搜索	▼ 条件	时间		·	
类型	主机	协议/主机帐户	用户	来源IP	开始时间/结束时间	会话时长/会话大小	操作
SFTP	192.168.1.110 CentOS	SSH root	张三 user01	10. 1	2018-04-20 09:55:25 2018-04-20 09:57:02	1分37秒 24KB	播放 下载 详情
SHELL	192.168.1.110 CentOS	SSH root	张三 user01	10. 1	2018-04-19 18:04:42 2018-04-19 18:06:12	1 分 30 秒 24KB	播放 下载 详情
SHELL	192.168.1.110 CentOS	SSH root	张三 user01	10. 1	2018-04-19 17:45:39 2018-04-19 17:47:09	1 分 30 秒 24KB	播放 下载 详情
SHELL	192.168.1.115 openSUSE	SSH root	张三 user01	10. 1	2018-04-19 17:34:19 2018-04-19 17:34:34	15 秒 24KB	播放 下载 详情

- 3. 选择会话日志,执行更多操作
 - 单击操作栏中的详情,可查看详细的会话信息,如图 12-96: 查看会话详情所示。
图 12-96: 查看会话详情

会话详情

×

会话ID	caaa10ee5593a83d000000292f00000f						
时长	34秒	大小	569KB				
开始时间	2015-07-01 16:43:41	结束时间	2015-07-01 16:44:15				
用户	hehe	来源IP	192.168.50.246				
来源MAC	00:50:56:8F:00:04	来源端口	50430				
主机名称	RD-server	主机IP	10.				
主机帐户	administrator	协议	RDP				
主机MAC	F4:EA:67:87:03:E7	主机端口	3389				
会话备注							
审批人	-	操作	播放 下载				

单击右上角关闭按钮,可返回会话审计页面。

• 单击操作栏中的**下载**,可将会话文件下载到本地。会话文件下载完成后,可通过离线播放器 进行播放。

➡ 说明:

在本地播放会话文件需安装离线播放器和Adobe AIR 4.0工具。单击云盾堡垒机系统页面右 上角的用户名,选择**工具下载**,可以下载离线播放器和Adobe AIR 4.0的安装程序。

单击操作栏中的播放,可通过Web方式查看会话审计回放。在线播放支持日志回放、命令记录、搜索等功能,如图 12-97: 查看会话审计回放所示。

通过Web方式查看会话审计,须要在本地安装Flash Player才可在线播放。如果本地客户端 未安装Flash Player,单击云盾堡垒机系统页面右上角的用户名,选择**工具下载**,下载并安 装Flash Player 12。

图 12-97: 查看会话审计回放

슻i	舌回放 (admin@192.168.27.89: SSI	4)	O 2015-04-03 11:06:17
		X Last login: Thu Apr 2 09:12:30 2015 from 192.168.27.71	
C:\		[usert@webprotector=22 ~]6 [usert@webprotector=22 ~]6 ls	
		[user@webprotector-22 -]\$ pwd /home/user	
		[Userewerprotector-22 -]\$ 11 total 0 [user@werprotector-22 -16	
	11:06:26 touch test		
	11:06:40 mkdir test		
	11:06:48 mkdir tests		
	共计 13 条记录		
	II » —•	00.00.04 /00.00.41 E	GB18030 ▼

关闭Web页面,即可返回**会话审计**页面。

12.3.4.2.1.2 搜索审计会话

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到审计 > 会话审计页面,选择所有会话,单击展开更多搜索条件,如图 12-98: 会话审计搜 家条件所示。

图 12-98: 会话审计搜索条件

协议	全部	~	时间		-	
主机	主机名称/主机IP					
主机帐户						
用户	用户名/姓名					
来源IP						
会话ID						
备注						
归档状态	全部	~				
删除状态	全部	~				
	搜索 ^ 收起更多搜索条件					

3. 根据需要设定搜索条件,单击搜索,查看符合条件的会话日志。

12.3.4.2.1.3 查询事件

操作步骤

1. 登录云盾堡垒机系统。

2. 定位到审计 > 会话审计页面,选择事件查询,查看会话事件,如图 12-99: 查看运维事件所示。

图 12-99: 查看运维事件

会话审计					
所有会话事件查询					
类型 图形文字		▼ 时间	Ð	-	
搜索	~ 展开更多搜索条	.(4			
时间	主机	用户	类型	内容	会话操作
2018-04-19 14:41:09	192.168.1.125	user01	图形文字	服务器管理器	播放 详情
2018-04-19 14:41:06	192.168.1.125	user01	图形文字	Windows 任务管理器	播放 详情
2018-04-19 14:40:58	192.168.1.125	user01	图形文字	Windows 任务管理器	播放 详情
2018-04-19 14:40:53	192.168.1.125	user01	图形文字	控制面板	播放 详情

3. 选择会话事件,执行更多操作。

- 单击会话操作栏中的详情,可查看详细的会话信息。
- 单击会话操作栏中的播放,可通过Web方式查看会话事件回放。在线播放支持日志回放、命令记录、搜索等功能,如图 12-100: 查看会话审计回放所示。



通过Web方式查看会话审计,须要在本地安装Flash Player才可在线播放。如果本地客户端 未安装Flash Player,单击云盾堡垒机系统页面右上角的用户名,选择**工具下载**,下载并安 装Flash Player 12。

图 12-100: 查看会话审计回放

슻	舌回放(a	admin@192.168.27.89: SSH ;)	9 2015-04-03 11:06:17
			Last login: Thu Apr 2 09:12:30 2015 from 192.168.27.71	
C:\			user@setprotector-22 -)6 [user@setprotector-22 -)6 1s	
			UserSwebprotector-22 ~ J6 pwd /home/user	
			lusersweeprotector-22 ~]\$ 11 total 0	
		touch test	[user@wedprotector-22 ~]\$	
) mkdir test		
		mkdir tests		
		3条记录		
	∎ →	•• -•	00.00.04 / 00.00.41	GB18030 -

关闭Web页面,即可返回**会话审计**页面。

12.3.4.2.1.4 搜索事件

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到审计 > 会话审计页面,选择事件查询,单击展开更多搜索条件,如图 12-101:事件查询搜 索条件所示。

图 12-101: 事件查询搜索条件

会话审计

所有会话	事件查询
类型	所有类型 时间 -
王机IP	王机名称/王机IP
用户名	用户名/姓名
会话ID	
山容光碑空	
内谷大健子	
	搜索 ^ 收起更多搜索条件

3. 根据需要设定搜索条件,单击搜索,查看符合条件的事件会话。

12.3.4.2.2 审计规则

审计规则是创建审计管理员与主机之间的对应关系,代表某审计管理员具有审计某主机的权限。

12.3.4.2.2.1 添加审计规则

操作步骤

- 1. 登录云盾堡垒机系统。
- 定位到审计 > 审计规则页面,选择事件查询,单击新建审计规则,打开新建审计规则页面,如图 12-102:新建审计规则所示。

图 12-102: 新建审计规则

新建审计规则

审计规则	
名称	
用户	主机
□ 删除 添加用户	副除添加主机

3. 单击**添加用户**,在**添加用户**对话框中勾选审计人员,单击**添加**,如图 *12-103*: 添加审计管理员所示。

图 12-103: 添加审计管理员

添加 首页 上一页 1/1 × 下一页 2 搜索用户名/姓名 Q 技角色过滤 admin 超级管理员	末页
2 搜索用户名/姓名 Q 按角色过滤 admin 超极管理员	
admin 超级管理员	×
✓ docauditor docauditor ait管理员	
doctest doctest 部门管理员	

4. 单击**添加主机**,在**添加主机**对话框中勾选被审计的主机,单击**添加**,如图 *12-104*: 添加被审计主机所示。

图 12-104: 添加被审计主机

添加主	添加主机 ×									
	添加	上一页	1/1 ~	下一页	末页					
C	搜索主机名/主机IP				Q					
	192.168.1.110 CentOS									
	192.168.1.115 openSUSE									
	192.168.1.120 windows									
	192.168.1.125 Windows服务器									
	192.168.1.3 192.168.1.3									

5. 填写审计规则名称,单击**创建审计规则**,即可通过该审计规则为选定的审计管理员赋予所选主机 的审计权限。

审计规则创建完成后,在**审计规则**页面,单击审计规则名称,可对该审计规则进行修改;勾选审 计规则,单击上方**删除**,可删除该审计规则。

12.3.4.3 运维报表

运维报表用于统计当前用户的运维信息。

12.3.4.3.1 按时间范围查看运维报表

操作步骤

- 1. 登录云盾堡垒机系统。
- 定位到运维 > 运维报表页面,选择用户,设置时间范围,查看运维统计信息,如图 12-105:查看运维报表所示。

送 说明:

选择页签,可查看不同类型的运维统计信息。

图 12-105: 查看运维报表

运维报表

日期: 2016-03-	30	- 2016-03-3	30	今天 昨天	本周 本月					导出报表 >
总览 运维次数	这 运维时长	活动时长	会话大小	字符命令数	传输文件数	来源IP访问数	运维时间分	'n		
总体				运维时长				活动时长		
运维主机数	0			总运维时长	0秒			总活动时长	0秒	
来源IP数	0			应用中心	0秒			应用中心	0秒	
				SSH	0秒			SSH	0秒	
运维次数				TELNET	0秒			TELNET	0秒	
				RDP	0秒			RDP	0秒	
总运维次数	0			VNC	0秒			VNC	0秒	
应用中心	0			FTP	0秒			FTP	0秒	
SSH	0			SFTP	0秒			SFTP	0秒	
TELNET	0			每日运维最早开始	时间			单次运维最长活动	时长0秒	
RDP	0			每日运维最晚结束	时间			单次运维最短活动	时长0秒	
VNC	0			单次运维最长时间	1 0秒			单次运维平均活动	时长0秒	
FTP	0			单次运维最短时间	1 0秒			每日运维平均活动	时长0秒	

3. 单击右上角**导出报表**,选择导出格式,可根据当前设置的用户、时间范围将报表以指定的格式导出到本地。

12.3.4.3.2 设置报表自动发送

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到运维 > 运维报表页面,单击页面右上角的报表自动发送。

在报表自动发送对话框中,设置发送周期,选择报表文件格式,开启报表自动发送功能,单击确定,如图 12-106:设置报表自动发送所示。

图 12-106: 设置报表自动发送

报表自动发送			×
如果开启了报表自 式发送给本部门的	目动发送,在1 的部门管理员和	辱个周期开始时,系统将会自动成成上一周期的运维报表,并以即 和审计管理员。	邮件形
状态	关闭	•	
发送周期	☑ 毎日	每日00:00发送	
	✔ 毎周	每周一00:00发送	
	☑ 每月	每月一日00:00发送	
文件格式	DOC	T	
确定			

启用报表自动发送功能后,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,并以邮件形式发送给部门管理员和审计管理员。

送明:

请确认相应的管理人员已在用户信息页面中设置邮箱信息。

12.3.5 系统管理员操作指南

12.3.5.1 登录云盾堡垒机系统

前提条件

请确认您所使用的客户端能够正常访问云盾堡垒机系统。

操作步骤

- 1. 打开Chrome浏览器。
- 2. 在地址栏中,输入云盾堡垒机系统的访问地址,按回车键(Enter),进入系统登录页面。
- 3. 在云盾堡垒机系统登录页面,输入系统管理员用户名、密码及验证码。

C		
E	说明	:

系统管理员的用户名及密码是由超级管理员所创建的。

4. 单击**登录**。

首次登录成功后,系统管理员需要修改密码。

12.3.5.2 系统管理

系统管理用于对云盾堡垒机系统自身配置进行管理。

12.3.5.2.1 管理网络相关设置

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到**系统 > 网络设置**页面。
- 3. 管理云盾堡垒机系统网络相关设置。
 - 选择网络设置页签,进行网络相关配置,如图 12-107: 网络设置页签所示。

图 12-107: 网络设置页签

月端保置 Web保置 基本推动 SMMP 12週3万年								
DNS信息		SSHORLINEIN						
創造DNS 10 目 開始DNS 10 目		554例口 24 启用 22						
		保存更改						
保存更改		接口信息						
协议第日		接口名称	速度	连进状态	IP地址	子间地码		
RDP 63389	8 息用	eth0	1000Mbps	~				
SSH 60022	* 日用							
TELNET 60023	* 启用							
VNC 5900	* 屈用							
SFTP 61022	* 日用							
FTP 60021	* 启用							
保持更改								

• 选择web设置页签,进行Web相关配置,如图 12-108: Web设置页签所示。

图 12-108: Web设置页签

网络设置 Web	设置 静态路由 SNMP IP源防护
Web设置	
_ شد ا_ ۱۸۷	40
WeDy两口	443
安全性	□ 增强HTTPS安全性 勾选后会使部分低版本浏览器无法访问系统,比如Windows XP系统的IE8及以下版本
保存更改	
Web证书配署	
系统IP	
保存更改	
自定义Web证书	
状态	未上传
证书主题	
证书	▲ 上传文件 仅支持PEM、DER格式证书
私钥	▲ 上传文件 仅支持RSA算法密钥
加密口令	没有加密口令请留空
证书链	▲ 上传文件 (可选项)包含多个PEM证书的文件

• 选择静态路由页签,设置静态路由规则,如图 12-109:静态路由页签所示。

图 12-109: 静态路由页签

新建路由规则 目的地址	网络设置	Web设置	静态路由	SNMP	IP源防护
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	新建路中圳	מח			
目的地址	初心主作口乃(
子网掩码 255.255.255.0 下→跳/网关	目的地	也址			
下跳/网关 出口设备 eth0 ▼ Metric 0 备注 創建路由规则 目的地址 子网掩码	子网络	奄码 255.	.255.255.0		
出口设备 eth0 ▼ Metric 0 备注	下—跳/网	列关			
Metric 0 日注 日 日的地址 子网掩码	出口谈	g备 eth	0		
	Me	etric 0			
创建路由规则 目的地址 子网掩码	音	 音注			
创建路由规则 目的地址 子网掩码					
目的地址 子网掩码	创建路由	规则			
目的地址 子网掩码					
	目的地址			子网掩	码

• 选择SNMP页签,设置简单网络管理协议及社团信息,如图 12-110: SNMP页签所示。

网络设置 Web设置 静态路由 :	SNMP IP: 题功却					
SNMP配置			新建只读社团			
状态 美田 系統玩识 DASUSM 物理位置 TestLocation 联系方式 admin@test.com	•		Read community SNIMPIE4: V2c IPRR/	•		
保行更改 家用节点信息			會讓社同 社团信息			
OID	名称	描述	社団	SNMP版本	IP限制	删除
.1.3.6.1.4.1.2021.4	memory	系统内存值息	test	v1	default	制脉
.1.3.6.1.4.1.2021.9	dskTable	系统进盘信息				
.1.3.6.1.4.1.2021.10.1.3	laLoad	系统CPU负载				
.1.3.6.1.4.1.2021.11	systemStatus	系统CPU信息				
.1.3.6.1.2.1.2	interfaces	系统网卡信息				
.1.3.6.1.2.1.4	ip	系统IP值息				
.1.3.6.1.2.1.6	tcp	系统TCP值息				

图 12-110: SNMP页签

• 选择IP**源防护**页签,选择防护模式并设置黑白名单IP列表,如图 12-111: IP源防护页签所示。

图 12-111: IP源防护页签

塔设置	Web设置	静态路由	SNMP	IP源防护		
本设置						
防护	莫式 白名	单模式		T		
保存更改	z					
名单IP列	表					
名单IP列	」表	白名单IP				
3名単IP列 1 1 1 1 1 1 1	山表 删除 添加 建素IP/地址/备	白名单印				

12.3.5.2.2 管理认证相关配置

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到**系统 > 认证管理**页面。
- 3. 管理云盾堡垒机系统登录认证相关配置。
 - 选择安全设置页签,进行登录安全相关配置,如图 12-112:安全配置页签所示。

图 12-112: 安全配置页签

安全配置 远标	呈认证 双因子认证						
登录配置 							
登录超时	30 分钟 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30。						
验证码	☑ 启用验证码						
	验证码过期时间 60 秒 有效值15-3600。如果设置为0,则不过期。默认60。						
限制	□ 禁止admin从Web登录						
保存更改							
用户锁定							
密码尝试次数	10 次 有效值0-999。如果设置为0,则不锁定帐户。默认值5。						
锁定时长	30 分钟 有效值0-10080。如果设置为0,则锁定帐户直到管理员解除。默认值30。						
重置计数器	5 分钟 有效值1-10080。登录尝试密码失败之后,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。						
保存更改							
用户密码配置							
密码策略	 ■ 使用强密码 8-64个可见字符,必须包含以下4项:1.大写字母A-Z;2.小写字母a-z;3.数字0-9;4.非字母符号如@,#,\$. ■ 新用户强制改密 本地认证用户首次登录系统后必须修改密码 						
密码使用期限	0 天 有效值0-999。如果设置为0,则密码不过期。默认值0。						

• 选择远程认证页签,进行远程认证相关设置,如图 12-113: 远程认证页签所示。

说明: 在远程认证页签,也可以选择关闭本地认证方式,仅通过远程认证方式登录云盾堡垒机系 统。

图 12-113: 远程认证页签

安全配置 远程	认证 双因子认证	E
本地订证		
49087.6L		
状态	开启	T
KETE WARE		
远程认证	AD	Y
	服务器地址	
	备用服务器地 址	
	端口	SSL SSL
	Base DN	
	域	
	帐号	
	密码	
	过滤器	例:(&(objectClass=person))
	同步选项	
	用户组	■ 同步用户所在组织单位为用户组
		□ 同步AD组为用户组并且同步组内的用户成员
	姓名	填写远程服务器上表示用户姓名的属性名,如:fullName,不保存请留空
	邮箱	填写远程服务器上表示用户邮箱的属性名,如:mail,不保存请留空
	手机	填写远程服务器上表示用户手机号码的属性名,如:mobile,不保存请留空
	测试连接	立即同步用户

• 选择**双因子认证**页签,设置双因子认证方式及短信配置,如图 *12-114*:双因子认证页签所示。



图 12-114: 双因子认证页签

安全配置 远程	以证 双因子认证	
双因子认证		
认证方式	 ※ 密码 ※ 手机APP令牌 ※ 提信口令 端在本页面下方配置 	
保存更改		
短信配置		
状态	阿里云短信服务 ▼	
	配置方法请参阅 阿里云短信服务文档	
	AccessKeyId	阿里云颌发给用户的访问服务所用的密钥ID
	AccessKeySecret	阿里云颁发给用户的密钥
	SignName	管理控制台中配置的短信签名(状态必须是验证通过)
	TemplateCode	管理控制台中配置的审核通过的短信模板的模板CODE(状态必须是验证通过)
	ParamString	json楷式,短偏验证码用\$smsToken代替
	测试手机号码 发送测试信息	

12.3.5.2.3 管理系统相关配置

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到**系统 > 系统配置**页面。
- 3. 管理云盾堡垒机系统相关配置。
 - 选择运维设置页签,进行运维相关配置,如图 12-115:运维配置页签所示。

图 12-115: 运维配置页签

运维配置	告蓉配置	语言和界面	功能设置	SSH KEY配置							
运维配置											
未授权登录 🔮 允许未授权登录											
	□ 收集未授权登录										
	□ 收集主机帐户的密码										
		自动创建运维规则	U								
1244-2			₩=→+0 \s								
这班生	∄來 □ 九	计使用用户咨询:	豆灰土机 ፲	師丁用尸相土机吻	与问唐丁AD/LDAP的场景						
	□ 允	许使用用户SSH和	A钥登录主机								
	☑ 允	许使用SSH-agen	t-forwarding方	式登录SSH服务器	适用于SSH服务器要求采用Publickey方式登录的场景						
SSH 强	録 🛛 允	许使用公钥登录									
	☑ 允	许使用密码登录									
	□允	许发送环境变量									
	•	发送运维用户信息	USM_USEF	RNAME	变量名称可自定义						
	•	发送运维来源IP	USM_SOURC	EIP	变量名称可自定义						
	🗆 Us	mshell使用命令很	宁方式								
运维时长阴	剥 □ 空	闲时长超过	30 分钟	时自动断开连接							

• 选择告警配置页签,进行系统操作告警相关配置,如图 12-116:告警配置页签所示。

图 12-116: 告警配置页签

运维配置 告答配置 语言和界面 功能设置 SSH KEY配置	
操作日志告答	
秋赤 关闭 ▼ 邮件告答 □ 低 □ 中低 □ 中 □ 中高 □ 高 Syslog告答 □ 低 □ 中低 □ 中 □ 中高 □ 高 保存更文	
邮件配置	Syslog配置
发送方式 SMTP ▼ 服务器地址 第□ 25 ■ SSL ※号	发送者标识 服务器IP 第口 514 发送房试款据
发送测试邮件	保存更改

• 选择**语言和界面**页签,可以设置云盾堡垒机系统的语言,如图 12-117:语言和界面页签所示。

图 12-117: 语言和界面页签

运维配置	告答配	置 语言	语言和界面		SSH KEY配置
语言设置					
系统词	吾言 [简体中文		٣	
保存更改					

•选择功能设置页签,可以开启报表自动统计功能,如图 12-118: 功能设置页签所示。

图 12-118: 功能设置页签

运维配置	告警配置	音言和界面	功能设置	SSH KEY配置					
収主白动体	招表自动统计								
10:42 (14)3/	报表日初励订								
开报表自 开报表自	1动统计后 1动统计后	, 可以提升报表页面 , 系统会在每日0点,[数据加载效率 后自动统计前	-周期的报表数据,	会消耗一定系	毛统CPU资源并持续	一定时间,	请按需设置	
ł	大态 7	干启	•						
保存更改									

• 选择ssn Key配置页签,可以设置云盾堡垒机系统使用的RSA、DSA密钥,如图 12-119: SSH KEY配置页签所示。

图 12-119: SSH KEY配置页签

运维配置 告誓	翻置 语言和界面	功能设置	SSH KEY配置	
DSA密钥				
系统DSA指纹	92:f6:5d:	CROKER THE	00.000	
系统DSA公钥	ssh-dss AAAAB3Nz	aC1kc3MAAACB	AJrE0sZ60B0DBws	ClP3xDjzr
上传新DSA私钥	3			
RSA密钥				
系统RSA指纹	6b:39:0c:	a school	al and a second	
系统RSA公钥	ssh-rsa AAAAB3Nz	aC1yc2EAAAAB	IwAAAQEAyqpgAKU	zNGGChA/X
上传新RSA私钥	3			

12.3.5.2.4 管理系统存储

操作步骤

1. 登录云盾堡垒机系统。

- 2. 定位到**系统 > 存储管理**页面。
- 3. 管理云盾堡垒机系统存储空间。
 - 选择**数据归档**页签,查看磁盘数据状态并设置录像归档配置,如图 12-120:数据归档页签所示。

说明

在数据归档页签,还可以配置录像自动删除规则或手动删除系统数据。

图 12-120: 数据归档页签

数据归档 录	像导出日志备份	
磁盘数据状态		
系统分区		.53GB
会适分区	50.57GB可用,共5	53.29GB
归档状态	0个已归档,共0个	,0个已删除
录像归档		
状态	开启	T
	时段 速度限制	0 - 0 每天进行录像归档的时段,有效值0-23 0 MB/s 限定录像归档时的传输速度,有效值0-100,如果设置为0,则不限制传输速度
	传输模式	FTP v
	服务器地址	
	· 」 用户名	21
	密码	
	路径	绝对路径或相对路径,并确保用户具有此路径的写入权限
		测试用户 /展开历史错误日志

• 选择**录像导出**页签,可以通过创建录像导出任务将系统已记录的指定范围内的运维会话录像 导出其它FTP服务器,如图 12-121:录像导出页签所示。

图 12-121: 录像导出页签

203	彩白档 录像导出 日志奋份					
	开始 暂停 删除				首页 上一页 1/1 × 下一	页末页
		全郎 *	全部 *			
	任务名称	执行方式/首次执行时间	秋志	创建时间/创建人	远程服务器	详细
	test2	立即执行	正在2年以 0/0	2018-01-31 19:35:37 admin	ftp	洋價
	test	立即执行	已完成 0/0	2018-01-31 19:33:43 admin	ftp	详情

选择日志备份页签,可以为系统操作日志和运维会话日志创建备份,并将备份文件下载至本地,如图 12-122:日志备份页签所示。

图 12-122: 日志备份页签

数据回档 录像导出 日志報行			
日志報会			
时间10回 -			
御注			
内容 ※ 操作日志 ※ 会議日志			
新編日志論的			
黄份列表			
保存时间	备注	文件大小	操作
2018-01-31 19:37:17	-	1.05KB	下数 删除
2018-01-31 19:37:17	-	1.04KB	下號 删除
2018-01-31 19:37:16	-	1.04KB	下數 删除

12.3.5.2.5 查看系统操作日志

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到**系统 > 操作日志**页面。
- 3. 选择操作日志配置页签,选择操作日志类型,为每类操作设置重要性,如图 12-123:操作日志配置页签所示。

云盾堡垒机系统为每种操作都设置了默认重要性。

图 12-123: 操作日志配置页签

操作日志配置		
登录日志	Y	
重要性	默认重要性	日志描述
低 ▼	低	登录系统
低	低	退出系统
中低 ▼	中低	登录系统,未知系统错误
中低 ▼	中低	登录系统,用户不存在
中低 ▼	中低	登录系统,有效期之外登录
中低 ▼	中低	登录系统,用户被锁定
中低 ▼	中低	登录系统,密码错误
中低 ▼	中低	登录系统,本地认证被禁用
中低 ▼	中低	登录系统,远程认证被禁用
中低 ▼	中低	登录系统,认证模式不匹配
中低 ▼	中低	登录系统,从禁止的IP地址登录
中低 ▼	中低	登录系统,禁止admin从Web登录
中低 ▼	中低	登录系统,在禁止的时间段登录
中低 ▼	中低	登录系统,连接远程认证服务器失败
中低 ▼	中低	登录系统,认证方式未启用

4. 选择操作日志页签,设置搜索条件,单击搜索,查看操作日志记录,如图 12-124:操作日志页 签所示。

图 12-124: 操作日志页签

操作日志	操作日志配置					
Bite						
	接索	导出日志				
重要性	时间	日志英型	日志内書	用户	来源IP	结果
商	2018-01-31 19:37:18	维护日志	下账日志费份文件: log_start_end_20180131_5a71aa6d6552a0.zip	admin	10.36.1.129	成功
商	2018-01-31 19:37:17	维护日志	盤份日志: 不限	ədmin	10.36.1.129	成功
商	2018-01-31 19:37:17	维护日志	督份日志: 不限	admin	10.36.1.129	成功
高	2018-01-31 19:37:16	维护日志	醫份日志: 不現	admin	10.36.1.129	成功
高	2018-01-31 19:37:16	维护日志	鲁份日志: 不限	admin	10.36.1.129	成功
商	2018-01-31 19:37:12	维护日志	备份日志:不限	admin	10.36.1.129	成功
商	2018-01-31 19:35:39	维护日志	执行会话暂份任务: [test2]. 成功	[system]	127.0.0.1	成功
商	2018-01-31 19:35:37	维护日志	创建会适备份任务: 会适时尚: 不限, 主机: 所有主机, 任务名称[test2], 执行时间:	admin	10.36.1.129	成功



单击**导出日志**,可将当前页面的操作日志记录以CSV格式文件导出到本地。

12.3.5.2.6 查看系统报表

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到系统 > 系统报表页面。
- 选择系统报表页签,设置时间范围和展现粒度,查看各方面的系统报表趋势图和详细数据,如图 12-125:查看系统报表所示。
 - 图 12-125: 查看系统报表



 选择报表导出页签,选择报表周期、起始时间、导出格式,单击导出系统报表,可将完整的系统 报表导出到本地。

12.3.5.2.7 维护本机系统

操作步骤

- 1. 登录云盾堡垒机系统。
- 2. 定位到**系统 > 本机维护**页面。
- 3. 对云盾堡垒机系统本机进行维护。
 - 选择系统管理页签,进行系统管理相关配置,包括系统时间、系统升级、重启或关闭设备等,如图 12-126:系统管理页签所示。

图 12-126: 系统管理页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收
系统时间					
×.	19:57:5 2018-01-31	9 星期三			
时间服务器	^특 time.wind	ows.com		□ 自动同步	
同步服务	器时间	同步浏览器	时间		
系统升级					
软件版本	v	3.0.764.300			
硬件版本	C	LOUD			
出厂时间	2	018-01-25			
上传系统	新级文件 统前备份运	行数据,并确	保升级文件包:	完整。	
系统工具					
重启设备	i 关闭	设备 恢复	夏出厂设置		

• 选择许可证页签,查看许可证信息或导入新的许可证,如图 12-127:许可证页签所示。

图 12-127: 许可证页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统
许可证信息	Į				
客户信息		CR. ORA			
授权类型					
授权功能		(and a large			
过期时间		internation in the	10.01		
维保时间		inform D	-		
序列号		10.00			
最大连接数	(2	200			
最大主机数	(2	200			
许可证管理	1				
申请许可证 如需申请许 生成系统	河证 , 请导 认证文件	出系统认证文	件,并与相关	人员联系。	
备份许可证 当得到有效		之后,将原有	的许可证导出	到本地备份保存。	
备份许可	ίĒ				
导入许可证 完成以上步 导入许可	骤之后,就 骤之后,就 证	可以将许可证	导入到系统。		

• 选择**资源监视**页签,查看云盾堡垒机系统实时系统资源使用情况,如图 *12-128*:资源监视页 签所示。

图 12-128: 资源监视页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志	网络诊断工具	系统诊断工具	系统警报	控制台SSH	3 9 0				
	+5	网络接收	R	格发送	供应设置	建盘写入									
СРО	内仔	(Mbit/s)	(M	1bit/s)	(MByte/s)	(MByte/s)									
10%	5%	0.01	0.0	01	0	0									
100%															
50%															
0%									- CPU	· 使用率 — 内存	表用率				
	(单位:MBa	t/s)													
1000															
500															
0										- Dis.					
(单位:MByte	z/s)									1.45				
200															
100															

 选择系统备份页签,设置系统配置自动备份,手动备份或还原系统配置,如图 12-129:系统 备份页签所示。

图 12-129: 系统备份页签

系统管理 许可证	证 资源监视	系统备份	系统同步推送	系统同步接收	调试日志	网络诊断工具
系统配置自动备份						
状态	开启		T			
	周期 保留备份数 下次执行时间 上次执行时间	2 60 2018-02-0 2018-01-30	天 有效值1-4 有效值1-180, 01 00:01:05 0 00:01:05	50 当自动备份数量超	过此限制时会的	自动删除最早备份
保存更改						
系统配置手动备份						
备注						
创建系统配置备	63					
系统配置还原						
上传系统配置文件	<mark>件</mark> 前先进行系统配置	备份,并确保	上传的备份文件完整	腔。		

 选择系统同步推送页签,设置系统配置推送功能,可将本系统的配置定期自动推送至其他云 盾堡垒机系统,如图 12-130:系统同步推送页签所示。

图 12-130: 系统同步推送页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志	Mź
开启系统配 增加目标设	置推送,系 备IP之后,	统将按照设定的 需要在目标设备	的推送周期向目 昏的系统配置招	目标设备推送本设备 6收选项里填写本说	韵系统配置。 音的推送密钥。		
系统配置推	送						
ł	大态 开	宿		v			
推送周	周期	分钟					
推送器	的					显示重置	
密钥创建即	间						
保存更可	坆						
添加推送目	标						
ź	S称						
目标	πIP						
Webj	売口						
添加目标	5						

选择系统同步接收页签,设置系统配置接收功能,接收其他系统向本系统推送的系统配置,如图 12-131:系统同步接收页签所示。

图 12-131: 系统同步接收页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志				
开启系统配置接收,系统将允许其他设备向本设备推送系统配置。 需要设置源设备的推送密钥。										
系统配置接	逊文									
ł	状态 开	启		v						
源设备图	密钥					显示				
保存更近	<u>ل</u>									
接收结果										
源设备IP										
上次接收时	间									
上次接收结	课									

选择调试日志页签,查看系统调试日志,并可将日志导出到本地,如图 12-132:调试日志页 签所示。

图 12-132: 调试日志页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志	网络诊
大团刷新	台口口字						
2018-01-29 1	6:41:52.095	320 [2196] [D	1] SDB: close	sdb(session-slave	-1) 0/0/0		
2018-01-29 1	6:41:52.095	394 [2196] [D 695 [2104] [D	1] SDB: close	sdb(session-live) (0/0/0		
2018-01-29 1	6:41:52.095	842 [2194] [D	1] SDB: close	sdb(:memory:) 0/	0/0		
2018-01-29 1	6:41:52.096	208 [2195] [D	1] SDB: close	sdb(session-maste	er) 0/0/0		
2018-01-29 1	6:41:52.098	451 [2195] [D	1] SDB: close	sdb(session-slave)) 0/0/0		
2018-01-29 1	6:41:52.098	3575 [2195] [D	1] SDB: close	sdb(session-live) (0/0/0		
2018-01-29 1	6:41:52.098	8749 [2194] [D	1] dworker[0) quit Nanatahan dalata	-		
2018-01-29 1	0:41:52.099 6:43:47.280	005 [2193] [D 568 [1950] [D	1] gworker <t< td=""><td>/ispatcher> deleter</td><td>u</td><td></td><td></td></t<>	/ispatcher> deleter	u		
2018-01-29 1	6:43:42.282	2674 [1951] [D	1] New dwork	(er[0]			
2018-01-29 1	6:43:42.282	948 [1951] [D	1] New dwork	ker[1]			
2018-01-29 1	6:43:42.285	6494 [1951] [D	1] New dwork	ker[2]			
2018-01-29 1	6:43:42.290)291 [1954] [D	1] SDB: open	sdb(index-live)			
2018-01-29 1	6:43:42.293	305 [1952] [D	1] SDB: open	sdb(:memory:)			
2018-01-29 1	0:43:42.293 6:43:42.293	818 [1952] [D 1200 [1054] [D	1] SDB: open	sdb(session-live)			
2018-01-29 1	6:43:42.297	667 [1953] [D	1] SDB: open 1] SDB: open	sdb(:memory:)			
2018-01-29 1	6:43:42.297	749 [1954] [D	1] SDB: open	sdb(index-master))		
2018-01-29 1	6:43:42.298	8072 [1953] [D	1] SDB: open	sdb(session-live)			
2018-01-29 1	6:43:42.298	366 [1952] [D	1] SDB: open	sdb(session-slave))		
2018-01-29 1	6:43:42.301	.676 [1953] [D	1] SDB: open	sdb(session-slave-	-1)	07000)	
2018-01-29 1	0:43:42.311 6:42:42 211	565 [1958] [D	1] license: ex	pired at 2037-12-3 atura 'ali-oom-basi	1 23:59:59 (21458 -'	87999)	
2018-01-29 1	6:43:42.312	701 [1958] [D	1] license: de	code license v2 ok	- (
2018-01-29 1	6:43:42.320	525 [1958] [D	1] cgroup: m	ount caroup ok			
2018-01-29 1	6:43:42.321	.297 [1958] [D	1] Proxy: (19	58) Running			
2018-01-29 1	6:43:42.325	5172 [1952] [D	1] SDB: open	sdb(session-maste	er)		
2018-01-29 1	6:43:42.325	5741 [1953] [D	1] SDB: open	sdb(session-maste	er) Manaira ana i	10	
2018-01-29 1	6:43:42.326	864 [1953] [D	1] SDB: COUN	t s@session-slave-: 2) Rupping	1/session-master 0	/0	
2018-01-29 1	6.43.42.320	029 [1902] [D	1] SDB: count	z) running t s@session-slave/	session-master 0/0	1	
2018-01-29 1	6:43:46.392	424 [1951] [D	1] settings ch	anged: recording-(ON	r	

• 选择网络诊断工具页签,可通过连通性检测测试云盾堡垒机系统与目标主机之间的连通情况

并进行诊断,如图 12-133:网络诊断工具页签所示。

图 12-133: 网络诊断工具页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志	网络诊断工具
连通性检测	1						
Ę	陸型 「	PING		T			
主机地	出						
		执行测试					

选择系统诊断工具页签,选择所需诊断的系统信息,可查看诊断日志,如图 12-134:系统诊断工具页签所示。

图 12-134: 系统诊断工具页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志	网络诊断工具	系统诊断工具
系统诊断								
综合信息	l	v						
loadavg MemTota MemFree Buffers Cached: SwapCac nr_inac nr_inac nr_acti Persona unused No bonc	: 0.10 0.0 1: 8061312 : 7279100 : 204844 172416 kt thed: 0 kB 2_pages 182 tive_anon 65 tive_file ve_file 48 lities : devices: 0 (ing infomation)	03 0.01 1/18 2 kB kB 8 19775 108 5839 45183 8973 <none> ations.</none>	8 20647					
下载诊断	和志							



单击**下载诊断日志**,可将当前系统信息日志下载至本地。

• 选择系统警报页签,可查看系统警报记录,如图 12-135:系统警报页签所示。

图 12-135: 系统警报页签



📋 说明:

针对系统警报信息进行检测排查后,可选择相关警报,单击**确认警报**,将该系统警报标识为 已确认。

• 选择控制台ssu公钥页签,可查看控制台SSH公钥信息,如图 12-136:控制台SSH公钥页 签所示。

图 12-136: 控制台SSH公钥页签

系统管理	许可证	资源监视	系统备份	系统同步推送	系统同步接收	调试日志	网络诊断工具	系统诊断工具	系统警报	控制台SSH公钥
控制台SSH	公钥									
指纹 d0:20:1a:										
控制台SSF	1公 ss 钥 ◀ 合SSH公钥	h-dss AAAAB	BNzaC1kc3MA	WACBANiJxRSmrqR	•					



单击**重置控制台SSH公钥**,可重新生成一对SSH密钥,系统会保存公钥并显示私钥的内容,但不会保存私钥,请妥善保管私钥。

12.4 数据库审计

数据库审计系统是一款专业、主动、实时监控数据库安全的审计产品。本系统采用有效的数据库审 计方式,针对数据库漏洞攻击、SQL注入、风险操作等数据库风险行为进行记录与告警。同时,通 过系统监控引擎可以定制不同的审计规则,例如信任、敏感和不审计语句等规则,从而有效地评估 数据库潜在风险,实时监控数据库用户的访问操作行为。

数据库审计系统具有以下七大特点:

1. B/S架构设计,使用简单

本系统采用B/S架构设计,操作使用简单,无需客户端,通过浏览器即可完成各项功能的使用。

2. Agent式部署, Agent只转发流量, 性能影响小

此种模式只需要在数据库端或应用端部署数据库审计系统的rmagent 插件。插件若部署在应用端则只能审计到应用访问数据库的操作;插件若部署在数据库端,进行相关配置后,能审计到通过 网络或本地回环访问数据库的操作。插件rmagent本身没有复杂的处理逻辑,只根据受保护数据 库设置情况转发数据流量,因而并不会对部署插件的服务器的负载产生过多影响。

3. 友好的人机交互,简单易用

本系统采用全新的人机交互操作模式,基于人性化、专业化和可用性三个层面设计产品界面。产品附加辅助型功能,采用页面向导和标注解析的方式帮助用户更加快速、熟练的掌握本产品,有效地完成数据库的监控与审计操作。

4. 规则制定简单快捷

为方便用户定制审计规则,本系统采用优先级由上而下的规则命中机制,从多个层面定义数据库审计规则。

5. 自动检测针对数据库漏洞的攻击

本系统具备针对数据库漏洞攻击行为进行检测的能力,应对多样的数据库漏洞。在没有漏洞补丁防护的前提下,数据库审计系统基于网络层级对数据库进行监控,避免数据库长期暴露在入侵风险的攻击下。

6. 细粒度审计数据库操作行为

本系统可实时监视数据库登录、访问行为,有效地实施审计策略。同时,本系统还提供强大的数 据库活动审计分析能力,从多个角度灵活呈现数据库的活动状态,帮助用户有效地执行安全策 略。

7. 审计结果查询分级处理, 面面俱到

本系统可进行单库(数据库)级和全库(数据库)级两个层的审计查询。采用多重页面钻取技术,逐层递进地引导客户完成审计日志的查询分析。在审计日志统计分析方面,本系统独创的综合性统计分析报表,基于日报、周报、月报等基础型业务报表(可定时推送),结合专项性的模式分析类报表,开启了数据库审计产品报表展现形式的新纪元。

12.4.1 快速部署指南

12.4.1.1 数据库审计系统部署

云盾数据库审计系统通过镜像方式部署在专有云Enterprise版平台上的ECS云服务器中。

操作步骤

1. 登录Apsara Stack控制台。

送 说明:

部署云盾数据库审计系统需要使用具有相关资源权限的用户进行操作。

- 2. 定位到云管控中心 > 云基础产品 > 云服务器,选择实例页签。
- 3. 单击创建实例,进入创建云服务器ECS页面,创建云盾数据库审计系统服务器。

a) 设置区域、配置基本配置、网络等信息,如图 12-137: 设置ECS实例配置属性所示。

♀ 区域	区域	cn-qiandaohu-sg-d01		
	*可用区	可用区a	• 0	
③ 基本配置	*部门	yundun	•	
	* 坝日	yundun	Ť	
① 网络	* 网络类型	经典网络 专有网络		
		yundun/vpc-5	▼ yundun_sw1/vsw 35	-
	*安全组	yundun_sg	•	
	配置私网IP:			
		当前虚拟交换机网段为: 172.16.0.0/16		

图 12-137: 设置ECS实例配置属性

b) 单击**选择实例规格**,选择8核16G类型的ECS实例规格,如图 12-138:选择ECS实例规格所示。



云盾数据库审计系统服务器必须使用8核16G的实例规格。

图 12-138: 选择ECS实例规格

	实例系	列:	系列三							
实例	I/O优	i/L:	1/0优化实例							
	实例规	格: 8核16 団请	GB ecs.n4.2xlarg 选择实例规格	e						
系列三										
通用网络	增强型	sn2ne :								
		2核 8GB ecs.sn2ne.larg	4核 16GB ecs.sn2ne.	klarge	8核 320 ecs.sn2	6B ne.2xlarge	12核 ecs.s	48GB m2ne.3xlarge	16核 64GB ecs.sn2ne.4xlarge	
通用型 n	14 :									
		1核 2GB ecs.n4.small	2核 4GB ecs.n4.large	4核 8 ecs.n4	GB 4.xlarge	8核 16GB ecs.n4.2xla	arge	16核 32GB ecs.n4.4xlarge		

c)选择**公共镜像**,选择**云盾数据库审计**镜像,并选择对应的版本,如图 *12-139*:选择数据库审 计系统镜像所示。

图 12-139: 选择数据库审计系统镜像

镜	镜像类型:	公共镜像	自定义镜像			
像	*公共镜像:	云盾数据库审计	•	云盾数据库审计 V3.0.0	•	

d) 添加一块大小为4096GB(4T)的数据盘,如图 12-140: 添加数据盘所示。

送 说明:	
云盾数据库审计系统服务器必须添加一块大小为4T的数据盘。	
图 12-140: 添加数据盘

	*系统盘:	SSD磁盘		•	40	GB		
存储	数据盘:	高效磁盘		•	4096	GB	□ 随实例释放 ①	□ 加密 ①
		田増加一块	您还可选配 3 块					

e)填写服务器密码、实例名称,单击**创建**,创建云盾数据库审计系统ECS实例,如图 12-141: 设置服务器密码、实例名称所示。

图 12-141: 设置服务器密码、实例名称

	设 <u>置</u> 密码:	立即设置创建后设置
密码	*登录密码:	请输入密码 8-30个字符,且同时包含三项(大写字母、小写字母、数字、特殊字符)
	*确认密码:	
实 例 名 称	实例名称:	如不填写,系统自动默认生成 2-114个字符,以大小写字母或中文开头,可包含字母数字、下划线和横杠
数量	申请数量:	1 台 最多可批量创建50台ECS,配置私网IP时不支持批量创建
提交		创建取消

4. 联系销售人员,申请云盾数据库审计系统正式版的License许可。

云盾数据库审计系统默认提供3个月的试用License。

12.4.1.2 登录云盾数据库审计系统

前提条件

- 请确认您所使用的客户端能够正常访问云盾数据库审计系统。
- 请确认您已经从云盾数据库审计系统部署人员处获得云盾数据库审计系统的访问地址。
- 请确认您已经从云盾数据库审计系统部署人员处获得用户名和密码。

用户	说明
sysadmin	系统管理员账 号 默认密码:F2AD03E67CC3014F0A
secadmin	安全管理员账号
sysauditor	审计管理员账号

操作步骤

- 1. 打开Chrome浏览器。
- 2. 在地址栏中,输入https://云盾数据库审计系统的访问地址,按回车键(Enter),进入系统登录页面。
- 3. 在云盾数据库审计系统登录页面,输入用户名、密码及验证码。
- 4. 单击**登录**。

首次登录成功后,用户必须修改密码。

12.4.1.3 数据库审计系统初始化

÷

12.4.1.3.1 前提条件

数据库审计产品由Agent和Web控制台两部分组成,在使用数据库审计系统之前需要开放下列端

Π.

源	目的	端口	备注
运维管理端	Web控制台	443	Web控制台HTTPS服 务通讯端口
Agent	Web控制台	9266	Agent与Web控制台之 间的通讯端口
运维管理端	Web控制台	22	Web控制台SSH服务通 讯端口

12.4.1.3.2 导入License文件

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 2. 定位到系统 > 证书管理, 如图 12-142: 证书管理页面所示。

图 12-142: 证书管理页面

云盾•数据库审计	▲ 监控
通知管理 安全管理	时钟设置 系统控制 证书管理
证书管理 ヘ	
证书状态	正常
证书类型	正式版
产品型号	Xsecure-12000-100
序列号	
数据库审计	数据库实例数(10) [注:1个数据库实例=1组(IP+Port)]
颁发对象	user
本期服务起始日期	2018年04月23日
本期服务终止日期	2018年07月23日
注:上传文件应为官7	► 浏览 土 上传 うLicense文件

3. 在**证书管理**页面,单击**浏览**,选择从销售人员处获取到的正式版License文件的存放路径,然后 单击**上传**。

校验通过后,您才可以正常使用云盾数据库审计系统。

12.4.1.3.3 添加被审计的数据库实例

云盾数据库审计系统支持对云服务器自建数据库实例和云服务商提供的云数据库实例进行审计。

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 在概况页面,单击添加数据库,如图 12-143: 添加数据库所示。

图 12-143: 添加数据库

云盾•数据库审计		🕰 概况	Ⅲ 报表	📽 配置	▶ 维护	
审计时长 00 _天 00 _{小时}		语句总量 🚺 风	险总量 🚺 今日说	吾句 🚺 今日风险	0	
● 最近30分钟 最近2小时	最近12小时 今天	天昨天本周上	周本月上月目	自定义		
风险分布 10	高风险	中风险 🧧 低风险	会话统计 10	新建会话数	失败会话数 — 活跃会试	舌数 10
5			5 -			5
0 10:30	10:40 10	0:50	0 -	0:30 10:40	10:50	0
+添加数据库						

3. 在添加数据库页面中,填写被审计的数据库实例的相关信息,单击保存,如图 12-144: 填写数据 库实例相关信息所示。

图 12-144: 填写数据库实例相关信息

添加数据库 ****尼卡尔	doc mysal				4#12		
<u> </u>	uuc_mysqi			□多地址	加 还		
数据库类型	MySql	¥	IP地址	192.168.10.13			
	(2206			11
数据库版本	5.6	Ŧ	靖山	3306		保存取消	
选择字符集	UTF8	Ŧ	实例名				
操作系统	Linux 64	•					
操作系统	Linux 64	Ŧ					

表 12-2: 数据库实例信息说明

参数	说明	
数据库名	为被审计的数据库实例指定一个名字。	
数据库类型	根据被审计的数据库实例的类型选择。	
数据库版本	可以手动选择或者由系统自动获取。输入数据库主机IP、数据库 主机端口、数据库实例名、用户名、密码,单击 确认 ,系统会	

参数	说明	
	自动获取数据库的版本(对于Oracle数据库同时会获取到字符 集)。	
IP地址	 云服务器(ECS)自建数据库:被审计数据库实例的IP地址。 云数据库(RDS)实例:被审计的RDS数据库实例的URL连接串。 	
端口	被审计数据库实例的端口号。	
实例名	仅Oracle与Postgres类型的数据库需要填写,其他类型的数据库可以不填写。	
描述	为被审计的数据库实例添加注释。	

数据库添加成功后,可以在**概况**页面下方的数据库列表处看到所添加的数据库的摘要信息,如图 12-145:数据库实例添加成功所示。

图 12-145: 数据库实例添加成功

invalued and invalue and in	▲ 沃加粉焊店			
計算 数据库个数 1 P地址个数 1 清输入关键字 Q doc_mysql 前				
唐库 数据库个数 1 P地址个数 1 清输入关键字 Q 清输入关键字 Q 清输入关键字 Q 前 成金_mysql 前 版会适 0 个 向気を 反 い な の の の の の の の の の の の の の の の の の の				
▲ doc_mysql 揃 諏会活 0个 钩压力 0条/s 沃 心总量 0条 钩总量 0条	牧据库	数据库个数 1	IP地址个数 1	请输入关键字 Q
doc_mysql 前 政会活 0 个 拘压力 0 条/s 天 抛总量 0 条 拘总量 0 条				
 (前) (訴会話 0个) (拘压力 0条/s) (沃 (協急量 0条) (词总量 0条) 	doc_mysql			
¹¹ (((((((((((((((((((
(新会話 01) (新会話 01				
向压力 0条/s 次天 0条 洞总量 0条	活跃会话	ሀተ		
天 Ne:20日本 0条 和意量 0条	语句压力	0 条/s		
1 0 条 約总量 0 条	今天			
	风险总量	0条		
	语句总量	0 条		
	全部			
1险总量 0条	风险总量	0条		
狗总量	语句总量	0条		
号信息 IP地址(1)	● 信息 IP地址(1)) 🕈 🖉 📋		

12.4.1.3.4 部署Agent程序

12.4.1.3.4.1 Agent程序部署位置

Agent程序需要部署到数据库或应用服务器上,用于获取访问数据库的流量,帮助审计系统对获取 到的流量实现分析审计。

- 服务器自建数据库实例: Agent程序需要部署在数据库所在的服务器上。
- RDS数据库实例: Agent程序需要部署在对应的应用服务器上。

12.4.1.3.4.2 自动部署Agent程序

自动部署Agent程序功能目前仅支持Linux系统的服务器。对于自建数据库实例,数据库所在的服务器必须使用Linux系统;对于RDS数据库实例,对应的应用服务器必须使用Linux系统。

操作步骤

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 在维护页面,选择Agent管理,单击Agent自动部署。
- 3. 在Agent自动部署对话框中,填写部署参数,如图 12-146: Agent自动部署所示。

图 12-146: Agent自动部署

Agent配置: □本地回环 () ●审计服务器	应用程序与数据库在同一台机器上) NP:	
目标服务器:	192.168.100.88,pwd,22 192.168.100.89,pwd,22	格式:目标IP,root密码,ssh端口
查看执行日初	ŧ	

表 12-3: Agent自动部署设置

参数	说明
本地回环	如果应用服务与数据库部署在同一台服务器中,在自动部 署Agent程序时,需要勾选 本地回环 。
审计服务器IP	审计服务器IP地址。
目标服务器	部署Agent服务器的信息,格式为:目标IP,root密码,ssh端 口。 如果需要部署多个目标服务器,每个服务器的信息后面,按回 车(Enter)换行。

- 4. 单击部署,即可将Agent程序自动部署到相应的服务器中。
- 5. Agent程序自动部署完成后,返回Agent管理页面,单击Agent部署配置。
- 6. 在Agent部署配置对话框中,输入已部署Agent程序的服务器IP地址,然后单击添加,如图 12-147: Agent部署配置所示。

送 说明:

- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地址 即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服务器 的外网地址。
- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。

图 12-147: Agent部署配置

Agent部	署配置	
序号	IP地址	操作
1	172.17.71.212	Ē
2	192.168.0.1	Û
3	192.168.0.111	<u>ش</u>
IP地址:	192.168.100.88 192.168.100.89 添加	
		关闭

12.4.1.3.4.3 手动部署Agent程序

12.4.1.3.4.3.1 Windows系统服务器部署Agent程序 12.4.1.3.4.3.1.1 应用服务与数据库部署在不同的服务器的情况

操作步骤

1. 使用安全管理员#secadmin#登录云盾数据库审计系统。

2. 在维护页面,选择Agent管理,单击下载Agent。

系统自动弹出Agent部署配置提示,且浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下载至本地。

3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。



- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地址 即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服务器 的外网地址。
- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- **4.** 将Agent程序(即rmagent.tar.gz文件)文件上传到需要部署Agent程序的服务器,并将其解压缩,如图 *12-148*: 解压Agent安装程序所示。

图 12-148: 解压Agent安装程序

📙 🗹 📙 🖛 i n	magent				-	
文件 主页	共享	查看				~ 🕐
$\leftarrow \rightarrow \cdot \uparrow$, → rmag	gent >		√ Ō	搜索"rmagent"	Q
📌 快速访问	^	名称 ^		修改日期	类型	大小
三 桌面	*	linux64		2017/10/31 16:01	文件夹	
下書		install.sh		2017/9/28 9:44	SH 文件	2 KB
▼ 下就	7	🔊 rmagent		2017/10/31 15:38	配置设置	1 KB
🚆 文档	*	🌀 Rmagent_Setup		2017/9/28 9:44	应用程序	39,462 KB
▶ 图片	*	stop_rmagent.sh		2017/9/28 9:44	SH 文件	1 KB
02-云数据库	转全全运					
03-云数据库	掌防火墙					
04-云数据库	軍計					
加密部署						
🗥 OneDrive			Z			

- 5. 打开解压后的Agent程序文件夹,双击运行Rmagent_Setup.exe程序文件。
- 6. 在Installer Language对话框中,单击OK,如图 12-149:选择语言所示。

图 12-149: 选择语言



7. 在rmagent1.0安装对话框中,单击下一步,直到Agent程序开始安装。



选择组件时,必须勾选VS 2015 Redistributable和WinPcap组件,如图 12-150: 选择组件所

示,在Agent程序安装过程中会自动运行相关组件的安装程序。

图 12-150: 选择组件

🌍 rmagent 1.0 安装		_		\times
选择组件 选择你想要安装 rmagent 1.0)的那些功能。			Valid
勾选你想要安装的组件,并解 续。	滁勾选你不希望安装的组件。	单击 [下一步	⊨(N)] ≇	ŧ
选定安装的组件:	 ✓ rmagent core VS 2010 Redistributal ✓ VS 2015 Redistributal ✓ WinPcap npcap 	描述 停悬你的鼠 组件之上, 它的描述。	标指针到 便可见到	
所需空间: 28.0MB	< >>			
Nullsoft Install System v3.0	b2、 〈上一步(P)]	下—步(N) >	取消	(C)

8. 所有组件及Agent程序安装完成后,重新启动服务器。

12.4.1.3.4.3.1.2 应用服务与数据库部署在同一台服务器的情况

操作步骤

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 在**维护**页面,选择Agent**管理**,单击**下载Agent**。

系统自动弹出Agent部署配置提示,且浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下 载至本地。 3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。

送 说明:

- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地址 即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服务器 的外网地址。
- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- **4.** 将Agent程序(即rmagent.tar.gz文件)文件上传到需要部署Agent程序的服务器,并将其解压缩。
- 5. 打开解压后的Agent程序文件夹,双击运行Rmagent_Setup.exe程序文件。
- 6. 在Installer Language对话框中,单击OK。
- 7. 在rmagent1.0安装对话框中,单击下一步,直到Agent程序开始安装。

送] 说明:

选择组件时,必须勾选VS 2015 Redistributable和npcap组件,如图 12-151:选择组件所

示,在Agent程序安装过程中会自动运行相关组件的安装程序。

图 12-151: 选择组件

🧊 rmagent 1.0 安装		_		×
选择组件 选择你想要安装 rmagent 1.0 的那些功能。				
勾选你想要安装的组件,并解除勾选你不希望安装的组件。 续。	単击〔	下一步	(N)] ≩	ŧ
选定安装的组件:	- 描述 信息作 组件 它的打	尔的鼠桃 之上,他 苗述。	示指针到 更可见到	<u></u>
所需空间: 27.8MB				
Nullsoft Install System v3.0b2(上一步(P)下	⊼—步()	r) >	取消	j(C)

8. 所有组件及Agent程序安装完成后,修改C:\Users\<用户名>\AppData\Roaming\rmagent \rmagent.ini文件,将其中#loopback=1一行中的 "#" 删除以解除注释,保存文件,如图 12-152:修改Agent程序配置文件所示。

图 12-152: 修改Agent程序配置文件

🥘 rmagent - 记事本 \times 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) [rms] server_host=192.168.232.181 #server port=9266 #device=eth2 #device=tap0, tap1 #buffer_size=200 #queue_size=800000 #pcap_file=e:\0_Download\rmagent.pcap #pcap_file_num=10 #pcapybuffer=4 loopback=1 #web_server_port=80 #nice=-20 \square

9. 重新启动服务器。

12.4.1.3.4.3.2 Linux系统服务器部署Agent程序 12.4.1.3.4.3.2.1 应用服务与数据库部署在不同的服务器的情况

操作步骤

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 在维护页面,选择Agent管理,单击下载Agent。

系统自动弹出Agent部署配置提示,且浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下 载至本地。

3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。



- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地址 即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服务器 的外网地址。
- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- 4. 以root用户登录需要安装Agent程序的服务器,将rmagent.tar.gz文件上传到服务器,并将其解压缩,如图 12-153: 解压rmagent.tar.gz文件所示。

图 12-153: 解压rmagent.tar.gz文件

[root@rsdsdf ~]# ls anaconda-ks.cfg install.log install.log.syslog [root@rsdsdf ~]# tar -xvf rmagenttar.gz	rmagenttar.gz
./	
./stop_rmagent.sh	
./Rmagent Setup.exe	
./linux64/	
/linux64/rmagent	
/magent ini	
/install_ch	
./ INStatt.SN	
[root@rsdsdf ~]#	

- 5. 执行chmod 755 install.sh命令,给install.sh文件增加权限。
- 6. 安装Agent程序, 如图 12-154: 安装Agent程序所示。

图 12-154: 安装Agent程序

```
[root@rsdsdf ~]#_./install.sh_
start rmagent ...
start rmagent success
[root@rsdsdf ~]# ^C
[root@rsdsdf ~]# _
```

7. 安装完成后,启动Agent程序(rmagent),如图 12-155: 启动Agent程序所示。

图 12-155: 启动Agent程序



12.4.1.3.4.3.2.2 应用服务与数据库部署在同一台服务器的情况

操作步骤

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 在维护页面,选择Agent管理,单击下载Agent。

系统自动弹出Agent部署配置提示,且浏览器自动开始将Agent程序(即rmagent.tar.gz文件)下 载至本地。

3. 在Agent部署配置对话框中,输入需要部署Agent程序的服务器IP地址,然后单击添加。



- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网,则直接添加内网地址 即可;如果与数据库审计系统不在同一个内网需要通过外网进行通信的,则需添加该服务器 的外网地址。
- 如果不添加部署Agent程序的服务器IP地址,审计系统将无法抓取该服务器的数据进行审计。
- **4.** 以root用户登录需要安装Agent程序的服务器,将rmagent.tar.gz文件上传到服务器,并将其解压缩,如图 *12-156:* 解压rmagent.tar.gz文件所示。
 - 图 12-156: 解压rmagent.tar.gz文件



- 5. 执行chmod 755 install.sh命令,给install.sh文件增加权限。
- 6. 安装Agent程序, 如图 12-157: 安装Agent程序所示。

图 12-157: 安装Agent程序



7. 安装完成后,进入rmagent安装目录,使用VI编辑器修改rmagent.ini配置文件,在文件最后加入 一行loopback=1,然后保存,如图 *12-158*: 修改*Agent*程序配置文件所示。 图 12-158: 修改Agent程序配置文件

server_host=60 loopback=1	
~	
~ ~	~
~	
~	
~	
~	
~	
~	
~	
~ ~	
~	
~	
~	
~	
~	
~	
~	
~	
~	
INSERT	

8. 执行./stop_rmagent.sh命令停止rmagent进程后,执行./rmagent命令重启Agent程

序,如图 12-159: 重启Agent程序所示。

图 12-159: 重启Agent程序



12.4.1.3.4.3.3 部署注意事项

Agent程序默认连接云盾数据库审计系统的内网IP,如果部署Agent程序的服务器与云盾数据库审计

系统之间通过外网连接则需要修改rmagent.ini中的IP地址。

12.4.1.3.4.3.3.1 Windows系统服务器修改Agent程序连接地址

- 1. 登录数据库所在服务器或RDS数据库实例所对应的应用服务器。
- 2. 找到并修改C:\Users\用户名\AppData\Roaming\rmagent\rmagent\rmagent.ini配置文件,将其中server_host一行的IP地址修改为云盾数据库审计系统的外网IP地址,保存文件,如图 12-160:修改Agent程序连接地址所示。

 \times

图 12-160: 修改Agent程序连接地址

```
magent - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
[rms]
server_host=60.
#server_port=9266
#device=eth2 
#device=tap0, tap1
#buffer_size=200
#queue_size=800000
#pcap_file=e:\0_Download\rmagent.pcap
#pcap_file_num=10
#pcap_buffer=4
#loopback=1
#web_server_port=80
#nice=-20
```

3. 重新启动rmagent服务。在服务管理器,选中Rmagent Service服务,单击重启动此服务,如图 12-161: 重启Agent程序服务所示。

图 12-161: 重启Agent程序服务

🔍 服务				×
文件(F) 操作(A) 查看(V) 帮助	(H)	3		
	ij			
Q 服务(本地)				
Rmagent Service	~ ^ ^ 名称	描述	状态	^
	🥋 Remote Access Auto Con	无论什么时候,当某个程序引用一个远程 DNS 或者 N		
停止此服务	🌼 Remote Access Connecti	管理从这台计算机到 Internet 或其他远程网络的拨号	正在运行	
重启动比服务	🌼 Remote Desktop Configu	, 远程桌面配置服务(RDCS)负责需要 SYSTEM 上下文的		
	🎑 Remote Desktop Services	允许用户以交互方式连接到远程计算机。远程桌面和远…		
	🆏 Remote Desktop Service	允许为 RDP 连接重定向打印机/驱动程序/端口		
	🆏 Remote Procedure Call (RPCSS 服务是 COM 和 DCOM 服务器的服务控制管	正在运行	
	🎑 Remote Procedure Call (在 Windows 2003 和 Windows 的早期版本中 , 远程	正在运行	
	Remote Registry	使远程用户能修改此计算机上的注册表设置。如果此服…		
	Rmagent Service		正在运行	
	Routing and Remote Acc	在局域网以及广域网环境中为企业提供路由服务。		
	🎑 RPC Endpoint Mapper	解析 RPC 接口标识符以传输端点。如果此服务被停止…	正在运行	
	🎑 Secondary Logon	在不同凭据下启用启动过程。如果此服务被停止,这种	正在运行	
	🎑 Secure Socket Tunneling	提供使用 VPN 连接到远程计算机的安全套接字隧道协	正在运行	
	🆏 Security Accounts Manag	启动此服务将向其他服务发出信号:安全帐户管理器(SA	正在运行	
	🆏 Security Center	WSCSVC(Windows 安全中心)服务监视并报告计算机	正在运行	
	🆏 Sensor Data Service	从各种传感器传送数据		
	🎑 Sensor Monitoring Service	监视各种传感器,以公开数据和适应系统和用户状态。…		
	🎑 Sensor Service	一项用于管理各种传感器的功能的传感器服务。管理传…	正在运行	
	© Server ≺	支持此计算机通过网络的文件、打印、和命名赞道共享	正在运行	>

12.4.1.3.4.3.3.2 Linux系统服务器修改Agent程序连接地址

操作步骤

- 1. 登录数据库所在服务器或RDS数据库实例所对应的应用服务器。
- 2. 进入rmagent安装目录,使用VI编辑器修改rmagent.ini配置文件,如图 *12-162:* 修改Agent程序配置文件所示。

图 12-162: 修改Agent程序配置文件



3. 将server_host的值修改为云盾数据库审计系统的外网IP地址,然后保存,如图 *12-163*: 修 改*Agent*程序连接地址所示。

图 12-163: 修改Agent程序连接地址

server_host=60.	
~	
~	
~	
~	
~	
~	
~	
~	
~	
INSERT	÷

4. 执行./stop_rmagent.sh命令停止rmagent进程后,执行./rmagent命令重启Agent程序。

12.4.1.3.4.4 部署测试

您可以通过已安装Agent程序的应用服务器访问被审计的数据库实例并执行SQL语句,然后使用安全管理员账号登录云盾数据库审计系统,查看是否有审计信息。

- 如果云盾数据库审计系统正常记录了该数据库实例的审计信息,则说明数据库实例部署成功。
- 如果云盾数据库审计系统未能记录到审计信息,请检查对应的Agent配置部署信息、Agent程序的服务进程和连接配置等。

12.4.2 系统管理员指南

系统管理员是云盾数据库审计系统的三大管理员之一,基于系统级别的操作对本系统进行统一的监控与管理。系统管理员可以监控系统性能、控制网络配置、管理系统升级和进行系统安全管理。 通过系统管理员(sysadmin)账号登录云盾数据库审计系统,如图 *12-164*:系统管理页面所示。

图 12-164: 系统管理页面

云盾·数据库审计	● 监控	🖵 系统				Z (2)	🛔 sysadmin 👻 🕞 退出
压力 资源与引擎 数据中心监控	异常日志 系统日志						
◎ 最近30分钟 最近1小时 最近2小时	最近12小时 今天 日	昨天 本周 上周 本月 _	上月 自定义				刷新
系统			— 内存 — CPU	流量			— 接收 — 发送
50%	15:55 11	,00 ¹ ,60 ⁵	16.10	50 0 1 15:45 15:50	1555 1600	1605	16.10 ¹
			已使用		可用	数总数	最后更新时间
交换分区 🖸 🛛 🕅 🕅					16.0	0G 16.00G	2018-01-10 11:54:32
系統分区 🕜	49%				19.7	2G 39.25G	2018-01-10 11:54:32
数据中心分区 🖓 🚺 🐂					254.2	8G 254.82G	2018-01-10 11:54:32
日志数据分区 🛛 🛛 🖗					96.0	96.00G	2018-01-10 11:54:32
数据采集分区 20%					31.7	6G 32.00G	2018-01-10 11:54:32
数据备份分区 20%					109.1	9G 109.21G	2018-01-10 11:54:32
					征中	状态 正常 系统	前间: 2018-01-10 16:14:23

云盾数据库审计系统为系统管理员提供以下两大功能模块:

- 监控模块:基于产品的系统层面,监控产品性能
- 系统模块:产品系统级配置

12.4.2.1 系统

系统管理员第一次登录云盾数据库审计系统后,需要进入系统模块完成相应的系统及配置。

12.4.2.1.1 证书管理

背景信息

证书管理页面,用于进行License的校验。只有在上传有效证书,且校验通过后系统才可以正常使用 云盾数据库审计系统。

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 2. 定位到系统 > 证书管理页面,单击浏览。

- 3. 从本地选择正式版License文件,单击打开,单击上传。
- 4. 证书上传且校验通过后,可查看证书信息,如图 12-165: 证书信息所示。
 - 图 12-165: 证书信息

云盾•数据库审计	▲ 监控		■(2) 🌢 sysadmin + 🕩 退出
通知管理 安全管理	时钟设置 系统控制 证书管理		
证书管理 ^			
证书状态	正常		
证书类型	正式版		
产品型号	Xsecure-12000-100		
序列号	10.00 P0.0		
数据库审计	数据库契例数(10) [注:1个数据库实例=1组(IP+Port)]		
派发对象	user		
本期服务起始日期	2018年01月08日		
本期服务终止日期	2018年04月08日		
注 <u>上</u> 修文体应为置) 件	E ØKK ▲ 上他 Litense文		
		证书状态 正	E常 系统时间: 2018-01-10 16:37:43

12.4.2.1.2 系统控制

背景信息

在系统控制页面,系统管理员可以管理数据库审计系统服务器。

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 2. 定位到系统 > 系统控制,管理数据库审计系统服务器,如图 12-166:系统控制页面所示。
 - 单击关闭系统,可关闭数据库审计系统服务器。
 - 单击重新启动,可重启数据库审计系统服务器。

图 12-166: 系统控制页面

云盾•数据库审计	88 监控	🖵 系统						🕿 (2) 🛔 sysadmin 🗸	☞ 退出
通知管理 安全管理 时钟设置	系统控制 证书管法	理							
(美) 美闭系统	(闭系统] 会将引擎设备	m¥关机							Â
C 重新启动 [[新启动] 会将引擎设备	¥关机并重新启动	3						
									•
						证书状态	下常	系统时间: 2018-01-10	16:37:10
送 说明:									

云盾数据库审计系统服务器关闭或重新启动期间,将无法提供任何功能,请谨慎操作。

12.4.2.1.3 时钟设置

背景信息

在**时钟设置**页面,系统管理员可以启用自动同步时间功能。不启用自动同步功能时,云盾数据库审 计系统默认使用系统当前时间。



自动同步功能默认为禁用状态。

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 2. 定位到系统 > 时钟设置页面,单击启用,如图 12-167:时钟设置页面所示。

图 12-167: 时钟设置页面

云盾•数据库1	iiit 20 #	註 ♀系统		≤() ≛sysadmin - ⊕ 退出
通知管理 安全	管理 时钟设置 系统控制	证书管理		
系统当前时 间: 自动同步	2018-01-10 16:40:18 ② 扇用 ⑧ 蔡用			
服务器1 地址 服务器时间 系统当前时间	获取NTP的间 6 ⁻ 获取NTP服务器时间失败!			
服务器2 地址 服务器时间 系统当前时间	正規(NTP3)前 1.centos.pool.ntp.org 2018-01-10 16:40:09 2018-01-10 16:40:10			
服务器3 地址 服务器时间 系统当前时间	<u>まれRCNTP時</u> 前 2. centos.pool.ntp.org 2018-01-10 16:40:09 2018-01-10 16:40:09			51 <i>00</i>
			1894 XX	Teretill, 2010 01 10 18:28:02

- 3. 设置时间同步服务器地址,单击获取NTP时间。
- 4. 服务器时间获取成功后,单击保存,即开启自动同步功能。

12.4.2.1.4 安全管理

背景信息

在安全管理页面,系统管理员可以设置DNS服务器配置以及网络访问配置。

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 定位到系统 > 安全管理页面,分别为WEB管理平台、SNMP、SSH、安全日志设置访问限制,如图 12-168: 网络访问设置所示。

图 12-168: 网络访问设置

20632058					
B管理平台访问限	制: 允许所有	٣	SSH访问限制: 允许所有 🔻		
IP列表		+	□P列表	+	
2始IP	终止IP	A	起始IP 终止IP	A	
		Ţ			
MP访问限制: 7	5元许 •		安全日志访问限制: (不允许 •)		
MP访问限制: 2	5 /11 7 •	+	安全日志功可限制: (不分)许 • • • • • • • • • • • • • • • • • • •	*	
MP访问限制: 7 PIP列表 ShiP	5 %许 •	+	 安全日本均均時期時: (不分け)・・) ● PP物数 ※回pP ※出P 	•	
MP访问段制: 7 PIP列表 2%IP	5 90年 •	•	安全日本均均明期(: 不分け ▼) ● P91% 記録P 図出P	•	
MP访问限制: 7 フロクリーズ こからい アクリーズ こからい アクリーズ こからい アクリーズ この の の の 見 り ・ 「 ス の の の 見 り ・ 「 ス の の の し の う し の う の し の う し の う し の う し の う し の う し の う し の う し の う し の う し の う し の う し の う し の う の の し の う の の の の の の の の の の の の の	556件 终止IP	•	史金日志切時期制: (不分) ・) → PP3数 200P 昭山P	•	
MP访问段制: 7 つ IP列表 23公IP	5%# 终止IP	•	全日本が10月期4: 万元19 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	•	

- 选择**允许所有**,即允许任何IP连接。
- 选择**不允许**,即不允许任何IP连接。



WEB管理平台访问限制无法设置为不允许。

• 选择IP**列表允许**,即只允许下方列表中的IP连接。单击IP列表右上方的添加按钮,可添加允 许访问的IP或IP段;选择已添加IP,单击删除按钮可删除该IP。

📕 说明 :

IP列表中的IP或IP段之间用英文分号(;)分隔,IP段用半字线符号(-)连接。例如,192.168.1.1-192.168.1.10;192.168.1.200-192.168.1.255。

3. 设置完成后,单击保存,网络访问设置即生效。

12.4.2.1.5 通知管理

背景信息

在**通知管理**页面,系统管理员可设置发送告警通知的Email服务器配置信息,并可以对Email配置信息的正确性进行验证。

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 定位到系统 > 通知管理页面,设置发送告警通知的Email服务器配置信息,如图 12-169:告警通 知管理所示。

图 12-169: 告警通知管理

云盾•数据库审计	🕰 监控 🖵 系统			☎ (2) 💄 sysadmin マ 🕩 退出
	置 系统控制 证书管理			
▲告警通知管理	Email设置入			
☑ Email设置	SMTP服务器地址:		用户名:	
	端口:	(1 - 65535)	密码:	
	加密连接类型: 无	Ŧ	发件人地址:	
	发信测试入收件人地址:	发送测试和片		禄 存

- 3. 填写完Email配置信息后,单击保存。
- 4. 填写收件人地址,单击**发送测试邮件**,可对Email配置信息的正确性进行验证。 如设置的收件人邮箱可收到测试邮件,表示Email配置信息正确。

12.4.2.2 监控

系统管理员具备对云盾数据库审计整体系统监控的能力,监控内容包括压力、资源与引擎、数据中心监控、异常日志、系统日志等信息。

12.4.2.2.1 压力

背景信息

在压力页面,展示云盾数据库审计整体系统压力分析的情况,主要包括两大区域:

• 区域一:根据指定时间周期或自定义周期查询系统压力情况

系统监控:内存、CPU使用情况,用于判断性能压力

流量监控:接收、发送的流量情况,用于判断网络压力

• 区域二:查询系统各分区使用情况

针对系统的交换分区、系统分区、数据中心分区、日志数据分区、数据采集分区、数据备份分区 等进行监控,并以百分比形式展现分区已使用情况。

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 2. 定位到监控 > 压力页面,选择时间周期,查看数据库审计系统的压力分析情况。

Ô		
	说明	:

单击刷新,可刷新当前压力页面的展示信息。

• 查看系统压力情况,如图 12-170:系统压力情况所示。

图 12-170: 系统压力情况



说明:

将鼠标移至系统监控图或流量监控图中,可查看该时间点的具体性能情况或网络情况。

• 查看系统各分区使用情况,如图 12-171:系统分区使用情况所示。

图 12-171: 系统分区使用情况

已使用	可用数	总数	最后更新时间
交接分区 ◎	16.00G	16.00G	2018-01-10 11:54:32
系统分区 0 49%	19.72G	39.25G	2018-01-10 11:54:32
数据中心分区 ◎ 0%	254.28G	254.82G	2018-01-10 11:54:32
	96.00G	96.00G	2018-01-10 11:54:32
数選采集分区 ♥ 0%	31.76G	32.00G	2018-01-10 11:54:32
数理备份分区 ● 0%	109.19G	109.21G	2018-01-10 11:54:32

12.4.2.2.2 资源与引擎

背景信息

资源与引擎页面,主要用于监控各引擎的运行状态及资源的使用情况。

操作步骤

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 定位到监控 > 资源与引擎页面,查看各引擎的运行状态及资源的使用情况,如图 12-172:引擎运行状态及资源使用情况所示。

📋 说明:

单击刷新,可刷新各引擎的运行状态及资源实时使用情况。

图 12-172: 引擎运行状态及资源使用情况



12.4.2.2.3 数据中心监控

背景信息

数据中心监控页面,用于监控数据中心的状态、最近十分钟入库记录数、运行时长、以及相关的会话信息等。

操作步骤

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 2. 定位到监控 > 数据中心监控页面,查看数据中心监控状态,如图 12-173:数据中心监控情况所示。



单击刷新,可刷新数据中心实时监控状态。

图 12-173: 数据中心监控情况

云盾•数据库审计	▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	➡ 系统				🛛 (2) 🛔 sysadmin ▾	🕞 退出		
压力 资源与引擎	記力 資源時間 数据中心监控 昇端日志 系統日志								
会话数:7	十分钟内入库记录数: 0 运	行时长: 0天4小时33分				2	3 刷新		
会话标识	客户端	客户端IP名称	命令	时长	状态语句	操作	*		
319	127.0.0.1:34076		Sleep	c		•			
320	127.0.0.1:34078		Sleep	C		•			
321	127.0.0.1:34080		Sleep	a		•			
322	127.0.0.1:34082		Sleep	a		•			
323	127.0.0.1:34084		Query	C		•			
1175	127.0.0.1:35822		Sleep	2		•			
1176	127.0.0.1:35824		Sleep	2		•			
							÷		
4							۱.		
					证书状本 正	一 至纯时间,2018-01-10 10	6:28:46		

选择监控会话,单击操作栏的结束会话按钮,可以终止该会话以释放资源。

12.4.2.2.4 异常日志

背景信息

异常日志页面记录了各个引擎的异常信息,用于分析排查系统异常错误。

操作步骤

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 定位到监控 > 异常日志页面,选择引擎名,单击查询,查看该引擎的异常日志记录,如图 12-174: 引擎异常日志所示。



选择引擎名时提示无数据,表示没有引擎出现异常。

图 12-174: 引擎异常日志

z	后•数据库审计	28 监控	系统			🐱 (2) 🔺 sysadmin 👻	🕩 退出	
压力	边 资源与引擎 数据中心监控 异常日志 系统日志							
3	리譯名: npp v 이							
文件	文件数量: 1							
	引擎名	开始时间	进程号	文件名	大小	操作		
	npp	2018-01-09 18:20:00	19806	core_INST_npp_20180109182000_19806.log	2.52K	📼 🗴 🖿		

- 3. 选择异常日志文件,可进行以下操作。
 - 单击操作栏中的查看按钮,查看异常日志文件详细信息。
 - 单击操作栏中的删除按钮,删除该异常日志文件记录。
 - 单击操作栏中的下载按钮,可将该异常日志文件下载到本地。

选择多个异常文件记录,单击右上方的批量下载、批量删除按钮,可将选中的异常日志文件批量下载至本地或删除。

12.4.2.2.5 系统日志

背景信息

系统日志页面记录了每个引擎运行期间的日志信息,包

括alw、gmon、im、npc、npp、smon、tlw、tman、dlp等引擎,日志类别包括error和info两种日志。

操作步骤

- 1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
- 定位到监控 > 系统日志页面,选择引擎、日志类别,单击查询,查看该引擎的系统日志记录,如图 12-175:引擎系统日志所示。

图 12-175: 引擎系统日志

云盾。数据库	审计 企 监控	🖵 系统			▼(2) 🛓 sysadmin マ 🕩 退出
压力 资源与引牌	擎数据中心监控异常日志系统	旧志			
引擎选择: tma	n v 日志类别: info	¥			Q查询
引擎名	开始时间	进程号	文件名	大小	操作
1 tman	2018-01-09 18:08:52	24882	INST_tman_20180109180852_24882.0	472.86K	*
2 tman	2018-01-08 22:01:12	12092	INST_tman_20180108220112_12092.0	444.79K	
3 tman	2018-01-08 18:59:27	4911	INST_tman_20180108185927_4911.0	80.84K	*
4 tman	2018-01-08 18:17:24	3217	INST_tman_20180108181724_3217.0	18.81K	٤
5 tman	2018-01-08 18:16:23	32306	INST_tman_20180108181623_32306.0	1.47K	*
6 tman	2018-01-08 18:04:33	26525	INST_tman_20180108180433_26525.0	6.29K	<u>*</u>
7 tman	2018-01-08 16:12:07	19887	INST_tman_20180108161207_19887.0	49.65K	<u>*</u>
8 tman	2018-01-08 15:58:50	9658	INST_tman_20180108155850_9658.0	6.69K	ž .
9 tman	2018-01-08 15:36:06	3151	INST_tman_20180108153606_3151.0	10.61K	<u>گ</u>
				证书状态	止常 系统时间: 2018-01-10 16:30:23

3. 选择日志文件,单击操作栏中的下载按钮,可将该日志文件下载到本地。

12.4.3 安全管理员指南

安全管理员(secadmin)是系统默认存在的用户,是监控、管理、制定审计安全策略的工作人员。

通过安全管理员登录数据库审计系统,如图 12-176:安全管理页面所示。

图 12-176: 安全管理页面

	000 m5/m Litt	S 152.01 Ve HCBE	▶ 理沪			🖀 (2) 🛔 secadmin 🖲
D 1	语句总量 764,25	2 风险总量 27	今日通句 64,683 今			
天小 1近30分钟 最近2小时 最近17	2小时 今天 附天 3	は周 上周 本月 上	1 自定义			
的布 10	■ 高风脸	中风脸 🧮 低风险	会话统计 10	■ 新建台送数 🔤 先效会送数 —)	10 SQL分布 10 10	DML DCL 🗮 🗮 🖄
			6			
12-04 12-11	12-18 12-2	5 01-01	0 12-04 1	2-11 12-18 12-25	01-01 12-04	12-11 12-18 12-25 01-01
数据库个数 1	IP地址个数	1 请能〉	笑健学 Q			
数据库个数 1 sqlserver	IP地址个数	1 请规	关键字			
数据库个数 1 sqtserver 会話 0 个 低力 0 多/s	IP地址个数	1 请能〉	关键字 Q			
	IP地址个数	1 (清晰)	关键字 Q			
t	IP地址个数	1 জিজ	父 聽字 Q			

数据库审计系统为安全管理员提供四大功能模块,包括概况、报表、配置、维护。

12.4.3.1 概况

概况页面由上而下分为两个区域,系统检测与数据库监控。

12.4.3.1.1 系统检测

背景信息

系统检测区域展示当前数据库审计系统的审计状态,包括审计时长、系统风险总量、SQL分布情况 等。

操作步骤

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 定位到概况页面,查看当前数据库审计系统的审计状态,如图 12-177:审计状态所示。

图 12-177: 审计状态

SC (2) La secadmin
活数 — 法获金活数 SQL分布 ■ DML ■ DCL ■ 再始终
10 10
5 5

- 审计时长:系统的审计时间,统计本系统自开始审计至今的总时长。
- 语句总量:本系统审计到的所有数据库语句总量。
- 风险总量:本系统所有数据库审计到的风险总量。
- 今日语句:本系统截止访问时间当日的审计语句量。
- 今日风险:本系统截止访问时间当日的风险总数。
- 3. 选择时间维度,查看风险分布、会话统计、SQL分布图。

送 说明 :

根据选择的时间范围,图形的统计粒度也相应调整。

风险分布:风险分布图基于高、中、低风险,以时间为单位统计某一时间范围内所有数据库
 总体风险分布情况。风险分布图采用动态展现形式,可以通过单击统计图例,根据统计需求
 动态展现风险分布情况,如图 12-178:风险分布图所示。

图 12-178: 风险分布图



- 会话统计:会话统计图基于新建会话数、活跃会话数等统计某一时间范围内会话数变化趋势。与风险分布图相同,在会话统计图中也可以通过单击统计图例,根据统计需求动态展现会话统计情况,如图 12-179:会话统计图所示。
 - 图 12-179: 会话统计图



- 新建会话数:指某一时间段内新建生成的会话数
- 活跃会话数:指某一时间段内同步产生的会话数
- SQL分布: SQL分布图,基于DML(数据管理)、DCL(数据控制)和其他操作分类统计某 一时间范围内SQL语句类分布情况。SQL分布图同样支持通过单击统计图例,根据统计需求 动态展现SQL分布情况,如图 12-180: SQL分布图所示。

图 12-180: SQL分布图



12.4.3.1.2 数据库监控

数据库监控区域,是针对当前系统审计所有数据库的汇总展示区域,可以一览当前数据库审计的全 貌。数据库列表汇总展现了每个数据库的审计信息,包括当前活跃会话、当前语句压力;今天风险 总量、今天语句总量;全部风险总量、全部语句总量,如图 12-181:数据库监控区域所示。



图 12-181: 数据库监控区域

12.4.3.1.2.1 添加数据库

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 2. 定位到概况页面,单击添加数据库,打开添加数据库页面,如图 12-182: 添加数据库页面所示。

图 12-182: 添加数据库页面

添加数据库 数据库名				□ 多地址	描述	
数据库类型	Oracle	*	IP地址			
数据库版本	9.1.0.0	•	端□	□ 动态		保存取消
选择字符集	ZHS16GBK	٣	实例名			
操作系统	Linux 64	٣				

3. 在添加数据库页面中,设置所需添加的数据库的相关信息,单击保存。

📕 说明:

添加SQL Server数据库时,还需要完成**会话识别配置**,输入具有一定权限的用户及其登录密码,单击**校验用户权限**,确认该用户有访问权限。安全管理员也可以单击**下载创建用户参考脚本**,根据参考脚本在相关数据库中创建特定用户用于数据库审计。

12.4.3.1.2.2 管理已添加的数据库

操作步骤

- 1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
- 定位到概况页面,在数据库列表区域,选择已添加的数据库,进行数据库的配置信息查看、修改 与删除等操作,如图 12-183:数据库列表操作所示。

图 12-183: 数据库列表操作

> sqlse	erver	
当前		
活跃会话		0个
语句压力		0 条/s
今天		
风险总量		0条
语句总量		64,683 条
全部		
风险总量		27 条
语句总量		764,252 条
€ 信息	IP地址(1)	5 🕑 🗎

单击已添加数据库的区块,上方系统检测区域的风险分布、会话统计、SQL分布图将只显示
 该数据库的审计状态;单击返回全数据库区域图按钮,则重新显示所有数据库的审计状

态。

单击信息,查看该数据库详细审计信息,包括审计时长、系统风险总量、SQL分布情况
 等,如图 12-184:单数据库详细审计信息所示。

图 12-184: 单数据库详细审计信息



关于单数据库详细审计信息的更多内容,参考数据库详细信息。



单击左上角数据库名称,选择全数据库即返回概况页面。

- 单击IP地址,查看该数据库IP分布情况。
- 单击修改按钮 , 可在数据库修改页面修改该数据库的相关配置信息,修改完成后单击保存即生效。
- 单击删除按钮 _____, 在弹出的信息提示对话框中单击确定, 即删除对该数据库的审计。

12.4.3.2 数据库详细信息

将数据库添加至数据库审计系统后,可查看该数据库的详细审计信息并为该数据库设置具体的审计 规则。 数据库详细信息页面包括概况(单库)、风险、语句、会话、报表、规则六大功能模块,并在页面 左侧展示该数据库的审计状态信息。

12.4.3.2.1 概况(单库)

数据库详细信息的**概况**页面根据选择的数据库显示该数据库单库的审计状态,并且显示的三个统计 图都支持超链接钻取,单击统计图中的具体时间点即可跳转到对应的页面查看详细审计记录。

- 风险分布图对应风险页面
- 会话统计图对应会话页面
- SQL分布图对应语句页面



数据库详细信息的**概况**页面中的SQL分布图采用双轴统计的方式,相比数据库审计系统**概况**页面 系统检测区域中的SQL分布图,增加了数据库SQL语句的响应时间,并以折现的形式展现,如图 *12-185*: 单数据库概况页面所示。

图 12-185: 单数据库概况页面



12.4.3.2.1.1 查看单数据库审计状态

操作步骤

1. 使用安全管理员#secadmin#登录云盾数据库审计系统。

- 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击信息,进入数据库详细信息页面。
- 3. 查看页面左侧的该数据库的审计状态信息,如图 12-186: 单数据库审计状态信息所示。
 - 图 12-186: 单数据库审计状态信息



单击数据库名称下拉菜单,选择数据库可以切换到不同的数据库详细信息页面。选择**全数据 库**,则返回数据库审计系统整体的**概况**页面。

12.4.3.2.1.2 查看单数据库详细信息概况

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到概况页面,选择时间范围,查看单数据库概况。



选择**自定义**,设置具体时间范围,单击**查询**,可查看自定义时间范围内该数据库的风险分布、 会话统计、SQL分布情况,如图 *12-187:* 选择时间范围所示。 图 12-187: 选择时间范围

◎ 最近30分钟 最近1小时 最近2小时 最近12小时 今天 昨天 本周 上周 本月 上月 自定义

12.4.3.2.2 风险

风险页面的主要功能是对被审计的数据库进行各种风险结果的查询及分析,主要包含敏感语

句、SQL注入、漏洞攻击、风险操作等风险。风险的统计结果与所设置的审计规则是息息相关

的,根据为该数据库所设置的审计规则产生相应的风险记录。

12.4.3.2.2.1 查看风险统计结果

背景信息

风险统计是对指定数据库某一查询周期内各类风险的统计概要说明,通过图表结构展现风险统计情况。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到风险 > 风险统计页面,选择时间范围,查看风险统计图表。

选择**自定义**,设置具体时间范围,单击**查询**,可查看自定义时间范围内该数据库的风险统计信息。

• 风险统计交叉表

图 12-188: 风险统计交叉表

风险统计 规则命中风险检索 ○ 今天昨天本周上周 本月												
序号	风险类别	高风险	中风险	低风险								
1	敏感语句	0	0	0								
2	SQL注入	0	0	0								
3	风险操作	27	0	0								
<												



单击表中的蓝色数值,可跳转至**规则命中**页面查看详细分析记录。

• 风险类别统计图

图 12-189: 风险类别统计图



送明:

风险类别统计图部分采用柱形展现各类风险分布情况,便于安全管理员进行直观分析。通过 单击统计图右上方的风险类别可控制是否显示该风险类别的统计数据。

12.4.3.2.2.2 查看规则命中记录

背景信息

基于对风险统计结果的延伸,**规则命中**页面展现每条风险记录命中规则的详细信息。安全管理员 在**规则命中**页面可以以时间为检索条件,逐一查询不同风险类别下不同风险级别的详细命中规则。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到风险 > 规则命中页面。
- 4. 设置查询时间范围,选择风险类别、风险级别,查看规则清单,如图 12-190: 查看规则清单所示。

说明:

输入风险名称,单击查询,可查看包含指定风险名称的规则清单。

图 12-190: 查看规则清单

云盾•数据库审计	∞8 概况 ▲风	险 \$语句	● 会话	Ⅲ 报表	\$ 8 规则	▶ 配置			≤ (2) 🛓 secadmin 👻 🗭 退出
Sqiserver → 数据库IP (2) 显示全部 マ	风险统计 规则命中 风险检索 ② 今天昨天本周上周 本	表 5月 上月 自定义							
■UNE 02 _天 18 _小	风脸类别:全部 數感语句 SG 风脸级别:全部 低 中 高 风脸名称:	QL注入 风险撮作							Q查询
语句总量 764,252	序号 规则名称			风险级别		变更时间	风险类别		命中数量
风险总量	1 高危操作行为			A		2018-01-08 15:50:35	风险操作		27
今日语句 0 今日风险 0	c								
							ETC:	出什太 正常	至绘时间, 2019 01 11 10:06:22

5. 查看详细信息。

• 单击规则名称,打开风险规则页面,查看该规则的详细信息,如图 12-191:查看风险规则详细信息所示。
图 12-191: 查看风险规则详细信息

名称 高危擾作行う 风险 ◎▲高 ○ 通知 □ 启用	为	2 启用								
🖵 IP地址					🔁 数据库	用户				· · · · · · · · · · · · · · · · · · ·
起始IP		结束IP			用	中名称			用户类型	
		无数据表示任意		•				无数据表示任意		•
田 数据库对象										
(数据库.)模式名	对象名		对象类型 对象范围							
		无数据表示任意		*						
 Ⅲ 操作 ● 登录 ● 全部 	操作 ≥ 指定操作								常用 全部	Q
数据定义 ・ A (DDL) × E 数据提纵 × U (DML) × C 数据控制	ALTER TABLE × CRE DELETE × DEL JPDATE × UPE GRANT	EATE TABLE × CRE LETE OUTPUT × INSE DATE OUTPUT × UPD	ATE USER V DROF RT × INSER ATETEXT	P DATABASE RT SELECT	✓ DROP TAE × MERGE	LE ×	MERGE OUTPUT	✓ TRUNCATE × SELECT	* UPDATE STATISTICS * SELECT INTO	
(DCL) 无WHERE 条件数据	操作 (整表数据操作,未指定表	玩不参与规则校验)			截图(Alt + /	0				
■无WHERE条件更	新数据 D 无WHERE条件	+删除数据								
影响行数限制	(适用于包	a含 SELECT、 UPDATE、	DELETE)							
排除客户端MAC 不	校验客户端MAC									
□范围 2018-0 2018-0	1-11 国日 清波 1-11 国日 清波	5择 ▼ 时至 5择 ▼ 时								-

 单击命中数量,打开命中列表清单页面,查看风险命中的详细信息。命中列表清单页面概要 说明了风险命中信息,并列举了风险发生的客户端IP、用户、执行数,如图 12-192:命中列 表清单所示。

图 12-192: 命中列表清单

	∞ 概況 ▲ 风险 \$ 语句	同 🗩 会话 🖬 报表 💐 規則	を配置	🖾 (2) 🛔 secad	lmin 👻 🕞 退出
sqiserver 数据库IP (2) 显示 审计时长	○ 风始快计 規制合中 风始快差 命中列表清单 携要: 2018-01-01 00:00:00~2018-01-31 23:59:59 + 风始	慢作 + 高危操作行为 + 高			
ᇦᅕᅟᆞ	客户端IP	客户端IP名称	用户	执行数	0 斎海
· 括句总量 时	1 60.		未知用户	21	
764,252	2 111		SA	6	命中数量
27 今日语句 0 今日风险 0	K ≪ 1 → K 【 函 当前页2条件 2条				
				关闭	

单击命中列表清单中的执行数,打开风险命中列表详情页面。风险命中详情页面上方的查询模板记录客户端IP、用户名称、风险类别、规则名称、风险级别、时间范畴以及"模糊查询"检索字段;下方的命中列表详细罗列了每条风险语句的触发时间、SQL、执行结果、影响行数、响应时间、风险等级,如图 12-193:风险命中详情页面所示。

图 12-193: 风险命中详情页面

客户端IP: 111.		客户端IP名 称:		数据库用户 名:	SA
风险类别: 风险操作		规则名称:	高危操作行为	风险级别:	A
时间: 2018-01-0 23:59:59	01 00:00:00 到 201	18-01-31		Q 查询 🛃 导出	
K « 1 » K 🗌 🖸) 当前页6条/共 6	条 条			
DROP TABLE MASTER.	DBO.TMP1120				
Ø 2018-01-08 20:38:18	≭成功]≡ 0	🗟 1995µs	A	5
DROP TABLE #ERR_LOO	i_TMP				
O 2018-01-08 20:32:56	≭成功	ķ ≣ 1	🗟 1243μs	A	5
DROP TABLE #ERR_LOO	5_TMP				
O 2018-01-08 20:32:56	≭成功	i ≡ 7	🖁 84375µs	A	E.
DROP TABLE #ERR_LOO	i_TMP				
O 2018-01-08 20:32:44	☎成功	j ≣ 7	🗟 784µs	A	5
DROP TABLE #TMP_PI	/OT_CONFIG_TABL	E			
Ø 2018-01-08 20:32:31	☎ 成功	j≡ 0	∑ 106404µs	A	5
DROP TABLE #TMP_PIV	/OT_CONFIG_TABL	E			
2018-01-08 20:32:31	≭成功	j≡ 0	2 91652µs	A	5

送明:

- 风险命中列表详情页面支持模糊查询,在查询框中输入关键字,单击查询,可查询特定的
 风险语句记录。
- 风险命中列表详情信息支持导出,单击**导出**,选择导出行数进行导出,如图 *12-194*: 导出 风险命中列表详情所示。

图 12-194: 导出风险命中列表详情

下载数据		×
导出大小: 100 导出范围: 1~100000		
	确定	关闭

导出的文件格式为csv,文件名默认为数据信息。

12.4.3.2.2.3 风险语句检索及处理

背景信息

风险检索是风险设置的核心组件,以列表清单的方式逐条展现风险语句的详情。风险语句的详细信息包括具体的SQL语句、(触发)时间、风险类别、风险名称、风险等级、数据库用户、客户端IP等。通过对检索到的风险语句进行设置,可将风险语句添加到信任规则、敏感语句或者不审计语句中。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到风险 > 风险检索页面,选择查询时间范围,查看风险语句记录,如图 12-195:风险语句检索所示。

图 12-195: 风险语句检索

J	风险统计	十规则命中 风	金检索									
() 47	天 昨天 本周 上周	本月上月自定	×.						▼祭件	: Q	查询
	检索条	牛为: 2018-01-01 00:00:0	0~2018-01-31 23:59:5	9				0 0	▼ 保存生效			
	序号	SQL语句	时间	风险类别	风险名称	风险等级	数据库用户	客户端IP	客户端IP名称	操作		
	1	DROP TABLE MASTE	01-08 20:38:18	风险操作	高危操作行为	A	SA	111		0 0) · ·	τ î
	2	DROP TABLE #ERR_L	01-08 20:32:56	风险操作	高危操作行为	A	SA	111				τ.
	3	DROP TABLE #ERR_L	01-08 20:32:56	风险操作	高危操作行为	A	SA	111		0 0	5	۲
	4	DROP TABLE #ERR_L	01-08 20:32:44	风险操作	高危操作行为	A	SA	111				τ
٢	5	DROP TABLE #TMP_P	01-08 20:32:31	风险操作	高危操作行为	A	SA	111		0 0	5	۲
	6	DROP TABLE #TMP_P	01-08 20:32:31	风险操作	高危操作行为	A	SA	111				τ
	7	ALTER TABLE [DBO]	01-08 19:39:02	风险操作	高危操作行为	A	未知用户	60.		0 0	5	τ
	8	ALTER TABLE [DBO]	01-08 19:38:38	风险操作	高危操作行为	A	未知用户	60.				τ
	9	ALTER TABLE [DBO]	01-08 19:38:30	风险操作	高危損作行为	A	未知用户	60.		0 0	5	τ
	10	ALTER TABLE [DBO]	01-08 19:36:46	风险損作	高危損作行为	A	未知用户	60.				T
	11	ALTER TABLE [DBO]	01-08 19:36:43	风险操作	高危损作行为	A	未知用户	60.)		0 0	>	τ
	12 M «	AITER TARLE IDROL	01-08 19:36:33 当前页27条/共 27条	风险遏作	高贵遏作行为	A	未知用户	60.		0 0		y v

- 4. 选择某条风险语句,进行处理。
 - 添加到信任语句。

单击操作栏中的设置为信任语句按钮,即可将该SQL语句设为信任语句,系统对该语句不再 作风险记录,如图 12-196:设置为信任语句所示。

图 12-196: 设置为信任语句



送] 说明:

单击风险语句列表上方的全部设置为信任语句按钮,可将当前列表中的所有SQL语句设为信任语句。

• 添加到敏感语句。

单击操作栏中的设置为敏感语句按钮,即可将该SQL语句设为敏感语句,系统将针对敏感风险进行告警,如图 12-197:设置为敏感语句所示。

图 12-197: 设置为敏感语句

ଁ ଓ	T	保存生效		лı		
客户端IP	客户站	IP名称	操作	Ξ		
111.		\rightarrow	0	8	T	Â
111.00.000.000			0	0	τ	
111.			9	8	T	
111.			0	0	T	
111.000.000.000			9	0	T	
111.			0	0	T	
60.2			0	8	T	



单击风险语句列表上方的全部设置为敏感语句按钮,可将当前列表中的所有SQL语句设为敏感语句。

• 设置为不审计语句。

单击操作栏中的设置为不审计语句按钮,即可将该SQL语句设为不审计语句,系统将不再审计该语句,如图 12-198: 设置为不审计语句所示。

图 12-198: 设置为不审计语句

0 8	▼ 保存生效	
客户端IP	客户端IP名称	操作
111	X	○○ ▼
111		9 0 T
111		00 T
111		S 8 T
111		0 0 T
111		0 0 T

送 说明:

单击风险语句列表上方的全部设置为不审计语句按钮,可将当前列表中的所有SQL语句设为 不审计语句。

5. 处理完成后,单击**保存生效**,根据风险语句设置的审计规则即时生效。

保存生效后,单击**导出报告**,单击**csv导出**,可将当前风险语句列表导出,如图 *12-199*: 导出风 险语句报告所示。

图 12-199: 导出风险语句报告



12.4.3.2.3 语句

语句页面记录了本系统审计到的所有数据库语句记录,基于语句分析可以清晰地对数据库访问的各类SQL语句进行分类查询、分析。云盾数据库审计系统支持的分析方式包括SQL统计、语句检索、模板检索、失败SQL、TopSQL、新型语句等。

12.4.3.2.3.1 查看SQL统计

背景信息

SQL统计是对指定数据库在某一查询周期内各类SQL语句的统计概要说明,通过图表结构展现语句 分布状态及语句来源统计。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到语句 > SQL统计页面,选择查询时间范围,查看操作类型及语句来源统计结果,如图 12-200: SQL统计页面所示。

图 12-200: SQL统计页面



• SQL操作类型分类统计

单击选择某操作类型,右侧的SQL操作统计图将以饼图的形式展示该操作类型的客户端IP分布情况,如图 12-201: 查看某操作类型/P统计图所示。

图 12-201: 查看某操作类型IP统计图



• 单击某操作类型的执行次数,可跳转至模板检索页面实现数据钻取。

• 语句来源分类统计

语句来源的分类方式包括客户端IP、数据库用户、工具三种分类统计形式,支持选择多项分类,并通过饼状图帮助安全管理员直观地了解分布情况。

例如,在客户端地址分类的基础上,勾选数据库用户、工具和应用分类,单击**查询**,如图 12-202: 查看某操作类型IP统计图所示。

图 12-202: 查看某操作类型IP统计图

选项:	☑ 客户端地址 🛛 数据库用户	9 ≥ 工具和应用 🧕 査询	圖导出文件			
序号	客户端地址	客户端IP名称	数据库用户	工具和应用	执行次数	客户端统计图 🕤
1	39.1		SA	无信息	424057 📤	
2	172		SA	MICROSOFT JDBC DRIVER F	303537	
3	60.1		SA	MICROSOFT SQL SERVER JD	21128	
4	60.1		SA	NAVICAT PREMIUM	10975	
5	172		未知用户	无信息	2444	
6	111		SA	MICROSOFT SQL SERVER MA	820	
7	172		未知用户	MICROSOFT JDBC DRIVER F	820	
8	60.1		未知用户	无信息	271	
9	111 🗰 🖬 🖬		未知用户	无信息	90	39.1 34 / 无信息
10	111		SA	jTDS	64	60. A / MICROSOFT SQL SERVER JOBC DRIVER
11	60.1		¢A.	NAVICAT DREMITIM	27	60.2 iA / NAVICAT PREMIUM 172 / 未知用户 / 无信意 其他

单击选择某条统计结果,右侧的统计图将以柱形图的形式统计该语句来源的SQL操作类型
 分布,如图 12-203: 查看某语句来源SQL操作统计图所示。

图 12-203: 查看某语句来源SQL操作统计图

选项: ≥客户端地址 ≥数据库	用户 🗷 工具和应用 查询	■ 导出文件				
序号 客户端地址	客户端IP名称	數据库用户	工具和应用	执行次数	SQL操作编计图	•
1 39.		SA	无信息	424057 📤	500k	
2 172		SA	MICROSOFT JDBC DRIVER F	303537		
3 60.		SA	MICROSOFT SQL SERVER JD	21128	400k	
4 60.		SA	NAVICAT PREMIUM	10975		
5 172		未知用户	无信息	2444	300k	
6 111		SA	MICROSOFT SQL SERVER MA	820	2004	
7 172		未知用户	MICROSOFT JDBC DRIVER F	820	2008	
8 60.		未知用户	无信息	271	100k	
9 111		未知用户	无信息	90		
10 111		SA	jTDS	64	Ok A A	
11 60		CA.	NAVICAT DREMITIM	27	SHEET. MADE HARDING	r

单击导出文件,可将当前语句来源统计结果导出到本地。

12.4.3.2.3.2 检索SQL语句

背景信息

在语句检索页面,安全管理员可以以时间为语句检索条件检索本系统审计的SQL语句。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到语句 > 语句检索页面,选择查询时间范围。
- 4. 单击**展开检索条件**,设置检索条件,单击检索。



单击**更多可选检索条件**,在**检索条件设置**对话框中,可添加更多检索条件。

5. 查看符合所设置的检索条件的语句。

语句列表以网格式报表的形式进行SQL语句检索分析结果。SQL语句分析项包括SQL语句、捕获时间、数据库用户、客户端IP、执行结果、影响行数等信息。

• 通过单击列表右上角的列设置按钮,可以选择列表项展示内容,如图 12-204:列表项显示设置所示。

图 12-204: 列表项显示设置

		● 更多可选检索条件	✔ 展开检索条件	Q检
				al II
客户端IP名称	结果	影响行数	● 序号	-
	成功	1	● SQL语句	
	成功	1	 ·	4
	成功	1	● 案户端IP	
	成功	1	● 客户端IP4	3
	成功	1	MACt地北	
	成功	1	● 结果	
	成功	1	 影响行数 	
	成功	1	 ● 响应时间 ● 物坛房 	_
	成功	1	146	
	र्ग ३३	1	143	
		1	144	
	र्ग्य यह	1	136	
	dTtta	1	524	
	5075	1	1/8	
	LIC-93	1	242	
		4	342	
		4	143	
		1	144	
	历纪-5月	1	8961	
	成功	1	159	
	成功	1	146	

- 单击导出报表按钮,选择csv导出,可将当前语句列表导出到本地。
- 6. 定位到某条语句,进一步查看该语句的详细信息。
 - 单击列表下方的**展开语句信息**,可概要地查看该SQL语句的相关信息,包括会话信息、客户端信息、服务器信息、SQL信息等。
 - 单击语句详情按钮,在语句详情页面查看该SQL语句的相关信息,包括访问来源、应用身份、SQL语句、受影响对象等,如图 12-205: 查看语句详情所示。

图 12-205: 查看语句详情

语句详情						
访问来源信息						
客户端IP:	172.17.71.235	端口:	42742	客户端IP名称:		
数据库用户:	SA	OS用户:	无信息	MAC地址:	EEFFFFFFFFF	
访问工具:	MICROSOFT JDBC DRIVER FOR SQL SERVER	主机名称:	无信息			
应用身份信息						
应用客户端IP:	N/A					
SQL语句信息						
SQL标识:	1	操作类型	: 数据操纵(E	ML)		
影响行数:	1	响应时间	: 153µs			
命中规则:	N/A	语句捕获	时间: 2018-01-10	0 11:55:15		
执行结果:	成功					*
受影响对象						
服务器IP:	172.17.71.212	端口:	1433	服务名 (实 例) :	ReportServer	
受影响对象:	N/A		截图(4	(lt + A)		*
SQL语句						
SELECT 1;						
						÷.

单击会话详情按钮,在会话详情列表中查看SQL语句所在通讯会话的会话信息以及此段会话
 中审计到的所有SQL语句概况,如图 12-206: 查看会话详情所示。

图 12-206: 查看会话详情

SERVER BURCH BIOLE ALL ALL ALL ALL ALL ALL ALL ALL ALL A	
SELECT 1;	
Q 2018-01-10 11:55:15 ×4 成功 ≔ 1	-

说明:

会话详情列表支持模糊查询审计到的SQL语句,并支持将会话详情列表导出到本地。

12.4.3.2.3.3 检索语句模板

背景信息

在**模板检索**页面可以对SQL语句模板进行查询。本系统采用语句模板的方式将SQL语句进行归纳整理,通过简化的SQL语句结构,对同一类SQL语句进行记录。安全管理员通过模板检索功能,可以快速定位高危SQL语句信息。

操作步骤

1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。

- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到语句 > 模板检索页面,选择查询时间范围,单击查询。



模板检索页面支持客户端IP、数据库用户、工具和应用、MAC地址、模板类型、Sql语句类型、 对象信息等查询条件。

- 4. 查看语句模板列表,包括模板语句、语句最后执行时间、执行次数等信息。
- 5. 选择列表中的语句模板,单击列表右侧的深度追踪按钮,可进一步查看该语句模板的信息,如图 12-207:深度追踪信息所示。

图 12-207: 深度追踪信息

深度追	踪			
摘要:	2018-01-01 00:00:00~2018-01-08 20:38:18 + DR(DP TABLE MASTER.DBO.TMP1120 + CREATE TA	ABLE + ALTER TABLE + DROP TABLE	
序号	客户端IP	客户端IP名称	用户	执行次数
1	111.		SA	1
M «	1 2 1 60 当前页1各/共 1条			

- 在语句模板列表,选择语句模板记录,在类型设置栏单击按钮可直接为该语句模板配置审计规则。
 - 单击操作栏中的设置为信任语句按钮,即可将该模板语句设为信任语句,系统对该类语句不 再作风险记录。
 - 单击操作栏中的设置为敏感语句按钮,即可将该模板语句设为敏感语句,系统将针对该类语 句作为敏感风险进行告警。
 - 单击操作栏中的设置为不审计语句按钮,即可将该模板语句设为不审计语句,系统将不再审 计该类语句。

单击语句模板列表上方相应的全部设置处理按钮,可为当前列表中的所有模板语句设置审计规则。

12.4.3.2.3.4 查看执行失败的SQL语句

背景信息

在**失败SQL**页面可以查看选定时间内所有执行失败的语句。针对失败SQL语句进行分析,帮助安全 管理员分析数据库可能存在的风险途径。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到语句 > 失败SQL页面,选择查询时间范围,单击查询。
- 4. 查看所设置时间范围内的执行失败的SQL语句列表。
 - 单击列表右上角的列设置按钮,可以选择列表项展示内容,如图 12-208: 失败SQL列表展示 列设置所示。

图 12-208: 失败SQL列表展示列设置

SQI	L统计	十 语句检索	模板检索 失败SC	L TopSQL	新型语句	访问源分析						
0	今天	、昨天 本周 。	上周本月上月自定	ŧ٧							▼条件 🤇	Q 查询
检测	素条件	‡为:2018-01-01 00	:00:00~2018-01-31 23:59:	59							● 序号	
J	茅号	发生时间	会话标识	客户端IP	客户端IP名称	数据库用户	操作系统用户	工具和应用	应答信息	SQL语	● 发生时间	
	1	01-09 18:56:29	2532201230021000000	39		SA	无信息	无信息	Could not find stored proce	SHOW TA	● 会话标识	
	2	01-09 18:39:46	2532189480021000000	39		SA		TSQL	Invalid object name 'dbo.a	SELECT (● 客户端IP ● 客户端IP 	A
	3	01-09 18:38:21	2532189480021000000	39		SA		TSQL	Unclosed quotation mark af	0[A0[B	 ● 各戶號IF石标 ● 数据库用户 	
	4	01-09 18:38:10	2532189480021000000	39		SA		TSQL	Invalid object name 'aaa'.	SELECT*I	● 操作系统用户	
<	5	01-09 18:37:46	2532189480021000000	39		SA		TSQL	Incorrect syntax near 'from	SELECT*	● 工具和应用	ΔА;
	6	01-09 18:37:25	2532189480021000000	39		SA		TSQL	Invalid object name 'aaa'.	SELECT*I		
	7	01-09 18:37:09	2532189480021000000	39		SA		TSQL	Invalid object name 'aaa'.	SELECT*	● <u>M</u> 督信息 ● SQL语句	۸
	8	01-09 18:36:00	2532189480021000000	39.		SA		TSOL	Incorrect syntax near 'sele'.	USE REP	ORTSERVER SELE	

• 选择失败SQL记录,单击会话标识,打开会话详情页面,查看该会话所执行的所有SQL语句,如图 12-209: 查看会话详情所示。

图 12-209: 查看会话详情

客户端IP/端口: 39	31652 客户	⊐端IP名称:	100000	操作系统用户:	无信息	
应用或工具: 元信息 时间: 2018-01-09 18:55:23	云 到 2018-01-09 18:5	5:42	Q 查询	▲导出		
	_					
K « 1 » 🕅 🗌 🖸	当前页1条/共1条					
K « 1 » K 🗌 G	当前页1条/共1条					
K « 1 » N G) 当前页1条/共1条					

• 选择失败SQL记录,单击SQL语句,打开语句详情页面,查看该语句执行的详细情况,如图 *12-210*:查看语句详情所示。

图 12-210: 查看语句详情

万石没住							
5.							
访问来源信息							
客户端IP:	39.	端口:	31652	客户端IP名称:			
数据库用户:	SA	OS用户:	无信息	MAC地址:	EEFFFFFFFFF		
访问工具:	无信息	主机名称:	iZ2zeamdl6me8	opnbt0jw7Z			
应用身份信息							
应用客户端IP:	N/A						
SQL标识:	2/2	操作类型:	过程调用				
影响行数:	0	则 <u>小V</u> 时1月:	1041µs				
命中规则:	N/A	语句捕获时间	쾨: 2018-01-0	09 18:56:29			
执行结果:	DB应答码: 2812、/	並答错误信息: Could	not find stored pr	ocedure 'show'.			
受影响对象							
服务器IP:	172.17.71.212	端口:	1433	服务名(实例):	ReportServer		
受影响对象:	N/A						
SQL语句							
SHOW TABLES	;						
语句模板					0 0	T	保存生效

• 单击列表右上角的导出报表按钮,选择csv导出,可将当前列表中的失败SQL语句信息导出。

12.4.3.2.3.5 查看TopSQL语句

背景信息

TopSQL页面,支持从平均耗时、耗时总量、执行次数维度针对数据库执行的语句信息进行查询排序,由大到小展示系统审计到的SQL语句。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到语句 > TopSQL页面,选择查询时间范围,单击查询。

送 说明:

TopSQL页面支持以下查询条件:

- 排序方式:平均耗时、耗时总量、执行次数
- Top统计数:10、50、100
- 分析内容:每分钟耗时大于**us,并且执行次数多于**次
- 4. 查看Top SQL语句统计表,如图 12-211: 查看Top SQL语句统计情况所示。

图 12-211: 查看Top SQL语句统计情况

云盾•数据库审计	& 成況 ▲风脸 \$语句 ● 会话 圖 报表 ✿。规则 ✔配置			🕿 (2) 🔺 sec	admin 👻 🕩 退出
sqlserver 🗸	SQL统计语句检索模板检索失败SQL TopSQL 新型语句 访问源分析				
数据库IP (2) 显示全部▼ 审计时长	○ 今天 昨天 本間 上間 本月 自定义			T	条件 Q 查询
66 66	检索条件为: 2018-01-01 00:00:00~2018-01-31 23:59:59 + 平均耗时排序 + TOP10				
	序号 SQL语句	SQL标识	执行次数	平均耗时(µs)	耗时总量(ms)
	1 SELECT '#+QUOTENAME(CAST(SERVERPROPERTY(N#)AS SYSNAME),#)+'#+'#+QUOTENAME(DTB.NAME,#)+'# AS [DATABASE_URN],D	215	1	2198021	2198
764,252	2 SET @IS_POLICY_AUTOMATION_ENABLED=(SELECT CONVERT(BIT,CURRENT_VALUE)FROM MSDB.DBO.SYSPOLICY_CONFIGURATION W	214	1	2198021	2198
风险总量	3 DECLARE @IS_POLICY_AUTOMATION_ENABLED BIT	213	1	2198021	2198
27	4 DROP TABLE #TMP_PIVOT_CONFIG_TABLE	196	2	99028	198
	5 SELECT '#+QUOTENAME(CAST(SERVERPROPERTY(N#)AS SYSNAME),'#)+'# AS [URN],CAST(SERVERPROPERTY(N#)AS SYSNAME)AS [N	195	2	99028	198
0	6 INSERT INTO #TMP_PIVOT_CONFIG_TABLE VALUES(@WDWINSTANCE,@WDWDATABASE,@ENABLED,@CACHEWINDOW,@CACHEDIRECT	194	2	99028	198
今日风险	7 CREATE TABLE #TMP_PIVOT_CONFIG_TABLE([MDWINSTANCE] SQL_VARIANT NULL,[MDWDATABASE] SQL_VARIANT NULL,[ENABLED] S	193	2	99028	198
0	8 SELECT @CACHEDIRECTORY=PARAMETER_VALUE FROM [MSDB].[DB0].[SYSCOLLECTOR_CONFIG_STORE] WHERE PARAMETER_NAME=	192	2	99028	198
	9 SELECT @CACHEWINDOW-ISNULL(PARAMETER_VALUE,0)FROM [MSDB].[DB0].[SYSCOLLECTOR_CONFIG_STORE] WHERE PARAMETER	191	2	99028	198
	10 SELECT @ENABLED=ISNULL(PARAMETER_VALUE,0)FROM [MSDB].[DBO].[SYSCOLLECTOR_CONFIG_STORE] WHERE PARAMETER_NAME	190	2	99028	198

- 单击列表右上角的列设置按钮,可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮,选择csv导出,可将当前列表中的Top SQL语句导出。

12.4.3.2.3.6 查看新型语句

背景信息

新型语句页面统计汇总了该数据库某一时间周期内审计到的新的语句模板,安全管理员可以查询系统审计到的新型语句的详细信息,并为新型语句指定审计规则。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到语句 > 新型语句页面,选择查询时间范围,单击查询。
- 4. 查看系统审计到的新型语句,如图 12-212: 查看新型语句所示。

图 12-212: 查看新型语句

云盾•数据库审计	∞ 概况 🛕 风险 💲 语句 🗩 会话 💷 报表 🛸 规则 🗡 配置		🛎 (2) 🛔 seca	dmin マ ເ⊕ 退出
Sqlserver 数据库IP (2) 最示全部▼ 审计时长	 ✓ SQL统计 语句检索 模板检索 失败SQL TopSQL 新型语句 访问源分析 ○ 今天 昨天 本周 上周 本月 上月 自定义 			【条件 Q 查询
02 _天 18 _小	場時通型 ◎ 常規語句 ◎ 不审计语句 ◎ 信任语句 ◎ 敏感语句 ◆ 更多条件信息			* *
语句总量	检索条件为: 2018-01-01 00:00~2018-01-31 23:59:59 * 常规语句		0 Ο Τ	保存生效 🦻
764,252	序号新型语句	首次执行时间	类型设置	
风险总量	1 SELECT UPPER(S.LOGIN_NAME), CASE WHEN(S.NT_DOMAIN IS NULL OR S.NT_DOMAIN=') AND (S.NT_USER_NAME IS NULL OR S.NT_USER_NAME=)THEN 01-10 10:43:51	0 0	τ ^
27	2 USE MASTER;	01-10 09:58:52		τ
今日语句	3 SELECT O. NAME FROM (REPORTSERVER).SYS.ALL_OBJECTS O INNER JOIN (REPORTSERVER).SYS.SCHEMAS S ON O.SCHEMA_ID-S.SCHEMA_ID W	HERE TY 01-09 19:13:33	0 0	τ
0	4 (SELECT O.NAME AS NAME,O AS NUMBER FROM [REPORTSERVER].SYS.ALL_OBJECTS O INNER JOIN [REPORTSERVER].SYS.SCHEMAS S ON O.SCH	EMA_ID= 01-09 19:13:29		τ
今日风险	5 SELECT V.NAME FROM [REPORTSERVER].SYS.ALL_VIEWS V INNER JOIN [REPORTSERVER].SYS.SCHEMAS S ON V.SCHEMA_ID=S.SCHEMA_ID WHER	E S.NAM 01-09 19:13:29	0 0	τ
0	6 SELECT O.NAME FROM [REPORTSERVER].SYS.OBJECTS O INNER JOIN [REPORTSERVER].SYS.SCHEMAS S ON O.SCHEMA_ID=S.SCHEMA_ID WHERE	S.NAME 01-09 19:13:29		τ
	7 SELECT NAME FROM [REPORTSERVER].SYS.SCHEMAS ORDER BY NAME	01-09 19:13:29	0 0	τ
	8 USE MASTER	01-09 19:12:34		τ
	9 SELECT*FROM MASTER.SYS.DM_EXEC_CONNECTIONS	01-09 19:05:37	0 0	٣
	10 SHOW TABLES;	01-09 18:56:29		τ
	11 SELECT COUNT(")FROM AAA;	01-09 18:55:46	0 0	۲
	12 SELECT NAME FROM SYSOBJECTS WHERE TYPE=#	01-09 18:45:03		τ -
	K 《 1 2 3 ≫ K GO 当前页100条/共 215条			
		证书状态 正常	案統时间: 201	8-01-11 10:45:59

📋 说明 :

在列表中单击语句,可查看该语句的详情。

- 5. 在新型语句列表中,选择语句记录,在类型设置栏单击按钮可直接为该语句配置审计规则。
 - 单击操作栏中的设置为信任语句按钮,即可将该语句设为信任语句,系统对该类语句不再作
 风险记录。
 - 单击操作栏中的设置为敏感语句按钮,即可将该语句设为敏感语句,系统将针对该类语句作 为敏感风险进行告警。

 单击操作栏中的设置为不审计语句按钮,即可将该语句设为不审计语句,系统将不再审计该 类语句。

单击新型语句列表上方相应的全部设置处理按钮,可为当前列表中的所有语句设置审计规则。

12.4.3.2.3.7 分析访问源

背景信息

访问源分析页面主要用于统计所访问数据库地址、数据库用户、客户端地址、工具和应用等信息。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到语句 > 访问源分析页面,选择查询时间范围,查看访问源分析结果,如图 12-213: 查看访问源分析结果所示。

送 说明 :				
勾选数据库地址、	数据库用户、	客户端地址、	工具和应用选项可显示相应维度的分析结果,引	٤
持多维度分析。				

图 12-213: 查看访问源分析结果

云盾。数据库审计	● 概况 ▲ 风险	\$语句 ● 会话	💷 报表 📽 规则 🗲 i	配置	■(2) 🌢 secadmin 🕶 👄 退出
sqlserver ▼ 数据庫IP (2) 显示全部▼ 审计时长	SQL统计语句检索模板检索 失败 〇 今天昨天本周 上周 本月 上月 选项: @ 数据库地址 @ 数据库用户 □	SQL TopSQL 新型语句 访问) 目定义 春户满地址 □工具和应用	原分析		查询 国导出文件
 ○2 天 18 小 市 市の总量 764,252 风始总量 27 今日活动 ○ 今日风险 0 0 	序码 数据库地址 1 172.17.71.212:1433 2 172.17.71.212:1433	 20回床用户 5A 未知用户 	执行次数 766622 3630	访问遵统计图	
				证书状态 正常	● 李号 1 ● 李号 2 系統时间: 2018-01-11 10.48.30

• 访问源统计表:根据所选择的分析维度,展示在查询时间范围内每个访问源的执行次数。

• 访问源统计图:通过饼图的方式直观地展示各访问源的占比情况。

12.4.3.2.4 会话

会话分析是对数据库的所有会话(Session)行为进行分类统计、分析和追踪,包括会话统计、会 话检索、失败登录、活跃会话、应用会话五个功能模块。通过会话分析功能,基于数据库通讯会话 进行线索分析,可以快速定位风险,提高数据库风险分析的效能。

12.4.3.2.4.1 查看会话统计

背景信息

会话统计页面对被审计数据库进行整体性的会话统计、分析。基于时间范围,根据客户端IP、数据 库用户、工具等维度统计新建会话数量信息。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到会话 > 会话统计页面,选择查询时间范围,单击查询,查看会话统计情况,如图 12-214:
 查看会话统计结果所示。

勾选客户端IP、数据库用户、客户端地址、工具选项可显示相应维度的会话统计结果,支持多 维度统计。

图 12-214: 查看会话统计结果

云盾•数据库审计	🕰 概況 🔺 风险	\$语句 ● 会话	■ 报表 📽 规则 🗲 配	置 (2) ≜ secadmin - I ● 退出
Mager Source State Sta	 	活跃会话 应用会话 L月 自定义 工具		Q查询
 ○2、 日 市 ロ ロ<th>序号 资户制P 1 172.17.71.235 2 111 3 60.7 4 39. 5 60.2 6 111</th><th> マージョンドング・ マージョンドング・ マージョン・ マージョン</th><th>新融会活政 306801 101 57 22 4 1</th><th>新建会话统计</th>	序号 资户制P 1 172.17.71.235 2 111 3 60.7 4 39. 5 60.2 6 111	 マージョンドング・ マージョンドング・ マージョン・ マージョン	新融会活政 306801 101 57 22 4 1	新建会话统计
				近土持大 正帶 系统时间。2019-01-11-10-49-50

• 新建会话统计表

根据所选择的维度,展示在查询时间范围内各个维度的新建会话数量。



单击新建会话数,打开会话详情页面,查看详细信息。

• 新建会话统计图

以饼状图的形式直观展现不同客户端IP、数据库用户、工具在新建会话中的占比情况。



新建会话统计图,支持动态展现、图形隐藏等功能,单击某个统计维度可在统计图中隐藏该 维度的信息,如图 12-215:新建会话统计图所示。



12.4.3.2.4.2 检索会话信息

背景信息

在会话检索页面,安全管理员通过可选条件可以分析会话信息。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到**会话 > 会话检索**页面,选择查询时间范围,单击**查询**,检索会话信息,如图 *12-216*: 会话检索页面所示。

图 12-216: 会话检索页面

云盾•数据库审计	2 8 概况	▲风险 \$语句	● 会话	■ 报表 🗳 规则	▶配置		Z (2)	🛓 secadmin 👻 📔 😁 退
Sqlserver .	会话统计 会话检索 失	败登录 活跃会话 应用	会话					
数据库IP (2) 显示全部▼ 审计时长	② 今天 昨天 本周 上周	本月上月自定义						▼条件 Q 查询
66 66	检索条件为: 2018-01-01 00:00	0:00~2018-01-31 23:59:59						al 🗆
	序号 会话标识	客户端IP 客户端I	P名称 数据库用	户 操作系统用户	工具和应用	登录时间	离开时间	停留(分)
	1 2532813110241000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377 ^
764,252	2 2532813110521000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
风险总量	3 2532813110141000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
27	4 2532813110181000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
今日语句	5 2532813110091000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
0	6 2532813110451000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
今日风险	7 2532813110081000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
0	8 2532813110151000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	9 2532813110061000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	10 2532813110231000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	11 2532813110551000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	12 2532813110201000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	13 2532813110271000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	14 2532813110351000	172.17.71.235	SA	无信息	MICROSOFT JDBC D	01-10 11:55:11		1377
	₩ « 1 2 3 4 5 6 7	8 9 10 11 12 »M	60 当前页100	条/共 10000条				
						证#	· 形状态 正常 系统时	间: 2018-01-11 10:52:00

📕 说明:

会话列表中的停留(分)指的是该会话的会话时长。

- 单击会话标识,打开会话详情页面,查看该会话的详细信息。
- 单击列表右上角的列设置按钮,可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮,选择csv导出,可将当前列表中的会话记录导出。

12.4.3.2.4.3 查看登录失败会话

背景信息

失败登录页面记录登录失败的会话信息,以网格式报表展现会话的相关信息,并统计失败总数。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到会话 > 失败登录页面,选择查询时间范围,单击查询,查看登录失败的会话信息,如图 12-217: 失败登录页面所示。

图 12-217: 失败登录页面

4	话统	+ 会话检索	失败登录 活時	天会话 应用会话						
0) 47	天昨天本周,	上周本月上月	自定义					т	条件 🤇 査询
	检索条	件为: 2018-01-01 (0:00:00~2018-01-3	1 23:59:59						
	序号	最后失败登录时间	客户端IP	客户端IP名称	数据库用户	操作系统用户	工具和应用	数据库应答	失败原因	失败总数
	1	01-10 03:48	49.		SA	无信息	OSQL-32	18456	用户 'sa' 登录失败。	198
	2	01-09 09:58	60.		SA	无信息	无信息	18456	用户 'sa' 登录失败。	1
	3	01-08 20:06	140		TEST	无信息	无信息	18456	用户 'test' 登录失败。	7
	4	01-08 20:06	14C		ADMIN	无信息	无信息	18456	用户 'admin' 登录失败。	7
	5	01-08 20:06	140		SA	无信息	无信息	18456	用户 'sa' 登录失败。	7
	K ≪	1 » 🕅 🗌 🕻	30 当前页5条/共 5	옾						

单击失败总数,打开失败登录清单页面,查看详细的失败登录记录,如图 12-218:失败登录
 清单所示。

图 12-218: 失败登录清单

要: 2018-01-01 00	:00:00~2018-01-10 03:48:00 + 4	49.4.135.15 + SA + 无信息	+ OSQL-32 + 18456				
序号 时间	客户端IP	客户端IP名称	数据库用户	操作系统用户	工具和应用	数据库应答	失败次数
1 01-10 03:48	49		SA	无信息	OSQL-32	18456	1
2 01-10 03:47	49		SA	无信息	OSQL-32	18456	24
3 01-10 03:47	49		SA	无信息	OSQL-32	18456	25
4 01-10 03:46	49 =		SA	无信息	OSQL-32	18456	52
5 01-10 03:46	49		SA	无信息	OSQL-32	18456	11
6 01-10 03:45	49		SA	无信息	OSQL-32	18456	41
7 01-10 03:45	49		SA	无信息	OSQL-32	18456	9
8 01-10 03:44	49		SA	无信息	OSQL-32	18456	34
« 1 » M	Go 当前页9条/共9条						

- 单击列表右上角的列设置按钮,可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮,选择csv导出,可将当前列表中的失败登录会话记录导出。

12.4.3.2.4.4 查看活跃会话

背景信息

活跃会话页面对某一时间段内较为活跃会话进行统计描述,以活跃会话趋势图、活跃会话统计表、 活跃会话统计图的形式进行展示。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到会话 > 活跃会话页面,选择查询时间范围,单击查询,查看所设定的时间范围内的活跃会 话情况,如图 12-219: 活跃会话页面所示。

图 12-219: 活跃会话页面



12.4.3.2.4.5 查看应用会话

背景信息

应用会话页面主要用于统计三层应用关联的会话审计信息。

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 定位到会话 > 应用会话页面,选择查询时间范围,单击查询,查看通过系统审计到的由应用创建 的会话情况,如图 12-220:应用会话页面所示。

ഹ		
	说明	:

单击条件,可设置应用相关的过滤条件。

图 12-220: 应用会话页面

	会话统	计会	话检索	失败登录	活跃会	话	应用会记									
	0 4	天昨天	本周	上周本月	上月	自定	×.								▼条件 🧧	Q查询
	检索器	餐件为: 2	018-01-0	1 00:00:00~20)18-01-31	1 23:59):59								.Id	
	序	弓 应用会	话标识		应用	用系统	IP	应用系统IP名称	応用用户	4	应用用户登录IP	首记录时间	尾记录时间		停留(s) 数据库用户	
									无数	据						
<																
	⋈ «	1 »		Go 当前页	0条/共 04	条										
_													证书状态	正常	系统时间: 2018-01-11 10	:55:14

- 单击列表右上角的列设置按钮,可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮,选择csv导出,可将当前列表中的应用会话记录导出。

12.4.3.2.5 报表(单库)

报表功能是审计日志大数据系统化分析的具体表现。利用审计报告、定时推送的报表功能将审计日 志和风险分析体系中所要求的数据库安全趋势以更加直观的形式进行展现,帮助安全管理员更加便 捷、深入地剖析数据库运行风险。

本章节主要介绍云盾数据库审计系统的数据库单库报表,即针对单个数据库的统计报表。

12.4.3.2.5.1 查看报表(单库)

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。

- 3. 定位到**报表**页面,选择报表类型,选择时间范围,单击**预览**,查看该数据库的单库报表,如图 12-221: 报表页面所示。
 - 图 12-221: 报表页面

云盾•数据库审计	企 概况	✿ 配置 ▶ 维	护					Z (()) 🛔 secadmir	i• ⊕i	昆出
□ 括 周报 月报 萨班斯报告 ○ 今天 昨天 自定义	PCI报告 客户端风险分析 客	户端工具应用分析报告 审计	录数统计报告 定	时推送	模板	类型 综合报	告	▼ 加入走	时推送任务	学出 预装	ŝ
日录 1 概述 2 风险分布状况 2.1 风险命中统计 2.2 常风险分布统计 2.3 常危规则命中清单 3 客户端统计分析 3.1 客户满地门的语句量统计分析(T 3.2 客户确全活转计(TOP20) 3.3 失败登录统计 3.4 失败登录统计	1 概述 2018年01月 被监控与审计的	5日.被审计的数据库有1个,客户数据库清单如下:	会状况报 ^{端共1个,使用的数据}	告-全 .	库	485次,高危风	险行为非	ŧ出现了15次;			
4 语句统计分析 4.1 按照访问类型分布	数据库名称	地址	数据库版本	客户端	会话总量	审计总量	风险	风险状况			
4.2 失败语句与成功语句 4.2 语句描版物 (G) (2020) # 2	数据库测试	192.168.242.101 : 3306	MySql 5.6	1	4	85	72	高危(15)			
1.3 日均常的小八A301日 4.4 平均耗时排名 5 性能状况 ▼	2 风险分布状况 2.1 风险命中统; 建: 乾计时间内	汁 ,被审计数据库产生的风险分布	青况。帮助用户多了自	平当前数据。	单的风险状态						
	敏感语句:明确 SQ1注入: 如注 凤险操作: 根据	有风险的语句执行情况,清重点: 入量过多,清明确信任规则是否; 定义的风险规则就计触发风险数;	关注; 充善,若不完善则有S 爱;	QL注入风险	·课航计的情况	;					-

- 报表类型:日报、周报和月报,萨班斯报告、PCI报告、客户端分析报告、风险登录分析报告 等。
- 报表内容:包括总体访问情况、风险分布、会话分布、语句分布、性能状况等。
- 统计图展现形式:包括饼状图、柱形图、条形图、双轴折线图等。
- 报表样例:例如,日报中的数据库访问压力统计报告,如图 *12-222*:数据库访问压力统计报告所示。

图 12-222: 数据库访问压力统计报告



4. 导出报表或为当前报表设置定时推送。

• 单击导出,选择导出格式,单击确定,可导出当前报表。



报表支持以Word、PDF、HTML格式导出。

单击加入定时推送任务,选择推送任务,填写报表名称,选择报表格式,单击确定,可为当前报表设置定时推送。

12.4.3.2.5.2 管理定时推送任务(单库)

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到报表页面,单击定时推送,管理定时推送任务。
 - 单击新增,在新增任务组对话框中,输入任务名称、邮件主题,设置发送周期、发送时间,勾选需要发送的用户,单击保存,可新增定时推送任务组,如图 12-223:新增定时推送任务组所示。

图 12-223: 新增定时推送任务组

云盾•数据库审计	(88 概况 🔒	□报表	📽 配置	ょ 维持	<u>ب</u>							S (0)	secadmin	▼ ເ+ 退出
日报 周报 月报 萨班斯报告	告 PCI报告	客户端风险分析	客户端工具	应用分析报告	审计记录	数统	计报告	定时推送							
	4主题 新	增任务组													
	tt										-	• 8			
缺省周发送任务定时	时发送报表	任务名称	任务名称			发送	类型		邮箱 td®db.com			8			
缺省日发送任务 定时	时发送报表	邮件主题	邮件主题				sysadmin		lidekui@dbse	c.com		8			
缺省月发送任务定时	时发送报表	发送周期	天 •				sysauditor					B			
		发送时间	请填写0~238	时点											
		启用	启用	•											
												-			
										保存	取消				
						_					_				

- 选择任务列表中的任务,单击右侧操作栏中的编辑按钮,可修改该任务组的相关参数,并可 启用或禁用该任务组。
- 选择任务列表中的任务,单击右侧操作栏中的删除按钮,单击确定,可删除该任务组。
- 选择任务列表中的任务,单击右侧操作栏中的任务列表按钮,可查看该任务组中的报表定时 推送任务,并且通过单击编辑和删除按钮,可以修改该任务的报告格式及任务名称,或删除 该推送任务。
- 选择任务列表中的任务,单击右侧操作栏中的发送历史按钮,可查看该任务组已发送报表的 历史记录。

12.4.3.2.6 规则

审计规则是云盾数据库审计系统的灵魂所在,系统正是通过所设置的审计规则完成对数据库的合规 审计。本系统的审计规则设置针对于指定的单个数据库,符合一个数据库一套审计规则的原则。

本系统提供优先级视图、分类视图两种规则划分方式:

- 优先级视图包括风险忽略、高风险、中风险、低风险等规则类型,通过多个等级的规则实现数据
 库的合规审计和告警功能。
- 分类视图包括风险操作、SQL注入、语句管理等分类,根据风险攻击来源定义审计规则。

表 12-4: 管理规则

视图	级别/分类	包括规则类型
优先级视图	风险忽略	优先级视图下管理信任语句优先级视图下管理信任规则

视图	级别/分类	包括规则类型
	高风险	 优先级视图下管理敏感语句 优先级视图下管理SQL注入规则 优先级视图下管理风险操作规则
	中风险	优先级视图下管理SQL注入规则优先级视图下管理风险操作规则
	低风险	优先级视图下管理SQL注入规则优先级视图下管理风险操作规则
分类视图	风险操作	分类视图下管理风险操作规则
	SQL注入	分类视图下管理SQL注入规则
	语句管理	

12.4.3.2.6.1 优先级视图下管理信任语句

对系统审计到的SQL语句进行定义,对于被设置为信任语句的SQL语句和操作,系统将予以放行,不进行风险审计处理。在信任语句列表中,安全管理员可以为语句重新定义审计规则。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角优先级视图。
- 4. 单击信任语句, 界面如图 12-224: 管理信任语句所示。

图 12-224: 管理信任语句

云盾·数据库审计	48 概况	🛦 风险	\$语句 ● 会话	■ 报表	✿ 规则	▶ 配置	■() 🌢 secadmin 🕶 🕀 退出
Not sqiserver	→ 规则						优先级视图 分类视图
数据库IP (2) 显示全部▼ 审计时长	风险忽略	模板举型	◎ 信任语句				Q 查询 更多条件信息
02 19	信任语句 (0) 信任规则 (0/0)	常用操作	× ALTER × CREATE × DE	LETE × DROP			
바	高风险						⊘ ③ ▼ 保存生效
语句总量 764,252	歌感培句 (0) SQL注入 (0/0)	序号 语句模板					类型设置
风险总量 27	风脸操作 (1/1) 中风险						
	SQL注入 (0/11) 风赊提作 (4/4)						
0	《低风险						
→DUD☆ 0	风险操作 (0/0)						
		K ≪ 1 ≫ M	Go 当前页0条/共 0条				

5. 在信任语句列表中,选择相应语句。

说明:
在信任语句列表上方,设置查询条件,单击查询,可查询特定信任语句。
6. 单击类型设置栏中按钮,设置信任语句、敏感语句、不审计语句。

7. 单击保存生效后,相应设置即生效。

12.4.3.2.6.2 优先级视图下管理信任规则

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角优先级视图。
- 4. 选择信任规则,单击新建规则按钮 , 进入新建信任规则页面, 如图 12-225: 新建信任规则所
 - 示。

图 12-225: 新建信任规则

▼ 规则							优先级视图	分类视图	2
风险忽略		名称 名称		☑ 启用			四 保存	● 返回	
信任语句	(0)	风险 💿 🗢 信任							
信任规则	(0/0)	不审计语句 □ 是							
高风险									
敏感语句	(0)	🖵 IP地址			+	5 数据库用户		8	1
SQL注入	(0/0)	起始IP	结束IP			用户名称	用户类型		L
风险操作	(1/1)	·			*			-	L
中风险			无数据表示任意			无数据表示	任意		L
SQL注入	(0/11)								L
风险操作	(4/4)								L
低风险					-			-	L
SQL注入	(0/2)	■ 数据库对象			6				L
风腔操作	(0/0)	(数据库.)模式名	对象名	对象类型 对象范围					L
		■操作	无数据表示任意		×			_	
									•

- a) 在**名称**中填写规则名称。
- b) 在IP地址、数据库用户、数据库对象和操作中填入规则信息。

根据信任规则,可设置对于指定客户端IP和数据库用户可以基于指定数据库对象(数据表、 视图等)执行指定的操作,系统不做风险审计和告警。

- c) (可选) 勾选**有**WHRER条件数据操作选项,设定信任规则只针对有where语句的SQL操作有效。
- d) (可选)单击高级设置的展开按钮,为信任规则设置具体的时间范畴,如图 12-226:设置具体时间范畴所示。

图 12-226: 设置具体时间范畴

🎤 高级						
排除客户端MA	C不校验客户端M	AC				
□范围	2018-04-24		B	请选择	•	时 至
	2018-04-24		B	请选择	۳	时
□ 毎月	请选择	Ŧ	号 至	请选择	¥	튝
□ 毎周	请选择	Ŧ	至	请选择	¥	
□ 每天	00:00:00		至	23:59:59		□分段
	00:00:00		至	23:59:59		

e) (可选) 对于已被定义为信任语句的SQL语句,可以设置是否不审计该语句,如图 12-227: 设置是否不审计该语句所示。

图 12-227: 设置是否不审计该语句

名称 名称	☑ 启用
风险 ● ♥ 信任	
不审计语句 🔲 是	

- f) 单击右上角的保存,保存信任规则。
- 5. 管理已存在信任规则。

表 12-5: 管理信任规则

操作	说明
复制	单击复制按钮,可将该规则的相关设置复制至 新建信任规则 页面,便于 安全管理员添加相似的规则。
移动	信任规则之间存在生效优先级,通过上移或下移按钮可以调整信任规则 的排序,顺序靠前的规则优先生效。
启用切换	单击启用或禁用按钮,可以设置是否启用该规则。
编辑	单击编辑按钮,可以修改该规则设置。
删除	单击删除按钮,可以删除该规则。

12.4.3.2.6.3 优先级视图下管理敏感语句

对系统审计到的SQL语句进行定义,对于被设置为敏感语句的SQL语句和操作,系统将根据所设置的审计规则记录风险并触发告警。在敏感语句列表中,安全管理员可以为语句重新定义审计规则。

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角优先级视图。
- 4. 单击敏感语句,进入管理敏感语句页面。
- 5. 在敏感语句列表中,选择相应语句。

送 说明:

在敏感语句列表上方,设置查询条件,单击查询,可查询特定敏感语句。

- 6. 单击类型设置栏中按钮,设置信任语句、敏感语句、不审计语句。
- 7. 单击保存生效后,相应设置即生效。

12.4.3.2.6.4 优先级视图下管理SQL注入规则

以列表形式展现系统当前已有SQL注入规则。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角优先级视图。
- 4. 单击SQL注入,进入管理SQL注入规则页面。

高风险、中风险和低风险中都包含SQL注入,请根据具体需求选择管理。

5. 单击新建规则按钮 🔔 , 定义新的SQL注入规则。

可设置对于包含指定SQL命令特征的指定SQL操作,判定为风险操作并进行告警,如图 12-228: 新建SQL注入规则所示。

图 12-228: 新建SQL注入规则

	☑ 启用			日保存	返回
通知 🔲 启用					
SQL命令特征 (AND关系)					
■ SQL注释 ■ OR关键词 ■ UNION关	键词 🔲 常量表达式 🕑 空密码验证				
⊞ 风险函数 (OR关系)				(I
(数据库.)模式名	对象名	对象类型	对象范围		
					¥
❤ 正则表达式 (用户自定义的正则表达式,要求表	达式符合PERL规范,输入的谓词必须大写)				Ţ
喙 正则表达式 (用户自定义的正则表达式,要求表)	达式符合PERL规范,输入的瞬间必须大写)				•
◆ 正则表达式 (用户自定义的正则表达式,要求表)	达式符合PERL规范,输入的谓词必须大写)				•

6. 管理已存在SQL注入规则。

表 12-6: 管理SQL注入规则

操作	说明
复制	单击复制按钮,可将该规则的相关设置复制至 新建SQL注入规则 页 面,便于安全管理员添加相似的规则。
启用切换	单击启用或禁用按钮,可以设置是否启用该规则。
编辑	单击编辑按钮,可以修改该规则设置。
删除	单击删除按钮,可以删除该规则。

12.4.3.2.6.5 优先级视图下管理风险操作规则

以列表形式展现系统当前已有风险操作规则。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角优先级视图。
- 4. 单击风险操作,进入管理风险操作规则页面。

高风险、中风险和低风险中都包含风险操作,请根据具体需求选择管理。

5. 单击新建规则按钮 💶 , 定义新的风险操作规则, 如图 12-229: 新建风险操作规则所示。

图 12-229: 新建风险操作规则

名称 名称		☞ 启用			四 保存	▶ 返回
风险 ● <u>A</u> 中 通知 □ 启用						
🖵 IP地址			+	5 数据库用户		ľ
起始IP	结束IP			用户名称	用户类型	
	无数据表示任意		* •	ħ	数据表示任意	•
Ⅲ 数据库对象			Ø			
数据库.)模式名	对象名	对象类型 对象范围				
	无数据表示任意		*			
			¥			
■操作 ■ 登录 ■ 全部	臨作 □ 指完攝作					

- a) 在**名称**中填写规则名称。
- b) 在IP地址、数据库用户、数据库对象和操作中填入规则信息。

根据风险操作规则,可设置对于指定客户端IP和数据库用户可以基于指定数据库对象(数据 表、视图等)执行指定的操作,进行风险审计和告警。

- c) (可选) 勾选**有**WHRER条件数据操作</mark>选项,设定风险操作规则只针对有where语句的SQL操 作有效。
- d) (可选)单击高级设置的展开按钮,为风险操作规则设置具体的时间范畴,如图 12-230:设置具体时间范畴所示。

图 12-230: 设置具体时间范畴

▶ 高级 📄						
排除客户端MA	C 不校验客户端M	AC				
□ 范围	2018-04-24		日	请选择	¥	时 至
	2018-04-24		日	请选择	•	时
□ 毎月	请选择	T	号 至	请选择	•	튭
□ 毎周	请选择	T	至	请选择	•	
□每天	00:00:00		至	23:59:59		□分段
	00:00:00		至	23:59:59		

- e) 单击右上角的保存, 保存风险操作规则。
- 6. 管理已存在的风险操作规则。

表 12-7: 管理风险操作规则

操作	说明
复制	单击复制按钮,可将该规则的相关设置复制至 新建风险操作规则 页 面,便于安全管理员添加相似的规则。
移动	风险操作规则之间存在生效优先级,通过上移或下移按钮可以调整规则 的排序,顺序靠前的规则优先生效。
启用切换	单击启用或禁用按钮,可以设置是否启用该规则。
编辑	单击编辑按钮,可以修改该规则设置。
删除	单击删除按钮,可以删除该规则。

12.4.3.2.6.6 分类视图下管理风险操作规则

通过风险操作页面可以针对高、中、低风险、信任等不同风险级别,进行分类查询和审计规则配置。 置。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。

- 3. 定位到规则页面,单击右上角分类视图。
- 4. 单击风险操作,进入管理风险操作规则页面。
- 5. 单击新建规则按钮 ___, 定义新的风险操作规则。
 - a) 在**名称**中填写规则名称。
 - b) 在**风险**中选择风险级别。
 - c)在IP地址、数据库用户、数据库对象和操作中填入规则信息。

根据风险操作规则及所选择的风险级别,可设置对于指定客户端IP和数据库用户可以基于指 定数据库对象(数据表、视图等)执行指定的操作,进行风险审计。

- d) (可选) 勾选**有**WHRER条件数据操作</mark>选项,设定风险操作规则只针对有where语句的SQL操 作有效。
- e) (可选) 单击高级设置的展开按钮,为风险操作规则设置具体的时间范畴。
- f) 单击右上角的保存,保存风险操作规则。

6. 管理已存在的风险操作规则。

表 12-8: 管理风险操作规则

操作	说明
复制	单击复制按钮,可将该规则的相关设置复制至 新建风险操作规则 页 面,便于安全管理员添加相似的规则。
移动	风险操作规则之间存在生效优先级,通过上移或下移按钮可以调整规则 的排序,顺序靠前的规则优先生效。
启用切换	单击启用或禁用按钮,可以设置是否启用该规则。
编辑	单击编辑按钮,可以修改该规则设置。
删除	单击删除按钮,可以删除该规则。

12.4.3.2.6.7 分类视图下管理SQL注入规则

通过对SQL语句进行特征描述,定义需要阻止的SQL注入语句或危险SQL语句。

背景信息

系统内建了部分SQL注入规则,安全管理员可以对内建规则的风险级别和是否启用进行设置,但无 法修改内建规则的内容。
- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**概况**页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角分类视图。
- 4. 单击SQL注入,进入管理SQL注入规则页面。
- 5. 单击新建规则按钮 ____,定义新的SQL注入规则。

可设置对于包含指定SQL命令特征的指定SQL操作,判定为风险操作并进行告警。

6. 管理已存在SQL注入规则。

表 12-9: 管理SQL注入规则

操作	说明
复制	单击复制按钮,可将该规则的相关设置复制至 新建SQL注入规则 页 面,便于安全管理员添加相似的规则。
启用切换	单击启用或禁用按钮,可以设置是否启用该规则。
编辑	单击编辑按钮,可以修改该规则设置。
删除	单击删除按钮,可以删除该规则。

12.4.3.2.6.8 分类视图下语句管理

安全管理员可以为语句重新定义审计规则。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到规则页面,单击右上角分类视图。
- 4. 单击语句管理,进入管理SQL语句页面。
- 5. 在语句列表中,选择相应语句。通过**类型设置**栏中的按钮将所选择语句设为信任语句、敏感语句、不审计语句。
- 6. (可选)通过选择**敏感语句风险**可为敏感语句设定风险级别。



在敏感语句列表上方,设置查询条件,单击查询,可查询特定敏感语句。

7. 单击保存生效后,相应设置即生效。

12.4.3.2.7 配置(单库)

12.4.3.2.7.1 配置单库的规则告警通知

背景信息

规则告警信息支持通过邮件的方式进行通知,便于相关管理人员及时了解数据库风险异常。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到概况页面,在数据库列表区域,选择已添加的数据库,单击**信息**,进入数据库详细信息页面。
- 3. 定位到配置 > 规则告警通知页面, 如图 12-231: 规则告警设置所示。

图 12-231: 规则告警设置

	● 概況 ▲ 5			🗩 会话			产配				2	(2) 📤 secadmin 🍷 📔 🕞 退出
Sqiserver → 数据库IP(1)显示全部 ▼										転業型 综合报告		
02 01 小 天 时 市 市 で64,252 27 今日明句 64,683 今日明政 0	日景 1 戦法 2 急体防闭循环 3 风险分布场况 3 风险分布场况 3 风险分布场况 4 金融分布场况 4 金融分布场况 4 金融分布场况 4 金融分布场况 4 金融分布场况 4 金融分布场况 5 3 面积和日中的计文观量 4 金融分布动力和 5 3 面积和日中的计文观量 5 3 面积和日中的计数 5 4 短端的可能和 5 4 短端的方面和一种的计数 5 4 短端的方面和一种的计数 5 4 短端的方面和一种的计数 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	系統告警	信息 型: ▼	恢复状 未恢	<i>के</i> : इ. ▼)	确认状态: 未确认 ▼]	▲ 登録 2018-01-08 15:57:18 2018-01-08 15:36:15 K ≪ 1 ≫ N ○ GD	告營共型 Agent异常 Agent异常		确 末 末	
				3 风险分 3.1 风服 注: 纪:	布状况 盘命中统计 计时间内,线线	8计数据库产生的5	(た分考试 当前圏	说,带动同户对了解查看就排 彩查询 超无数 据	"岸的风险状态		刻	

4. 勾选需要通过邮件通知的管理人员。



修改管理人员的邮件地址,需使用管理员账号登录后,单击右上角的账户名,在下拉菜单中选择**用户资料**,在**用户资料**对话框中即可进行修改。

5. 填写邮件标题,在文本框中输入邮件内容。

单击文本框上方的危险事件类型、服务器IP、服务器端口等参数,可将这些变量信息添加至邮件 内容中。

6. 填写最短告警周期,即最短多少分钟内发送一次系统告警邮件通知,单击确定。

12.4.3.3 报表

数据库审计系统采用聚集式报表展现形式,将报表分为全局报表、数据库单库报表两种表现形式。

本章节主要介绍数据库审计系统的全局报表,关于数据库单库报表说明,参见报表#单库#。全局报 表式以聚合报表的展现形式,分栏展现系统内所有数据库的审计状态报表。报表形式分为日报、周 报、月报,以及萨班斯报告、PCI报告、客户端风险分析、客户端工具应用分析报告、审计记录数 据统计报告等报表。同时,数据库审计系统提供定时推送功能,可将报表定时发送至指定人员的邮 箱。

12.4.3.3.1 查看报表

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 定位到报表页面,选择报表类型,选择时间范围,单击预览,查看全局报表,如图 12-232: 报表 页面所示。

云盾•数据库审计	🏾 概況		\$ 配置	▶ 维护						₩ (0) 👗 secadmi	n ▼ 0	◆退出
	告 PCI报告 客户辦	讽险分析 客户	端工具应用分析报告	审计记录数统计报	吉定	时推送	模板	类型 综合报	告	• DDA	韵推送任务	导出 1 8	列 克
日录 1 郵送 2 风险分布统咒 2.2 氮化设分布统计 2.3 氮化规分布统计 2.3 氮化规分布统计 3 客户满统计分析 3.1 客户满统时分析 3.1 客户满线时间都自量统计分析(T 3.2 客户声会运统计(TOP20) 3.3 失败登录统计 3.4 失败道导统计	1 概过	2018年01月18 被监控与审计的数	5日.被审计的数据库有 据库清单如下:	综合状 11个,塞户端共1个,使	兄报		库	共85次,高危风	顺行为非	共出现了15次;			
4 语句统计分析 4.1 按照访问类型分布		数据库名称	地址	数据	车版本	客户端	会话总量	审计总量	风险	风险状况			
 4.2 失败语句与成功语句 4.3 语句模板执行次数排名 		数据库测试	192.168.242.101	I : 3306 Mys	ql 5.6	1	4	85	72	高危(15)			
4.4 平均耗时排名 5 性能状况	2 风险	分布状况											
	2.1)	风险命中统计											
		註: 統计时间内, 敏感语句: 明确有 SQ1注入: 如注入 风险操作: 根据定	被审计数据库产生的 _尽 风险的语句执行情况, 量过多, 请明确信任却 义的风险规则统计触发	风险分布情况。帮助1 清重点关注; 见则是否完善,若不9 炎风险数量;	户多了解 善则有SC	(当前数据) QL注入风险	单的风险状态 x误统计的情况	L;					•

图 12-232: 报表页面

• 报表类型:日报、周报和月报,萨班斯报告、PCI报告、客户端风险分析、客户端工具应用分析报告、审计记录数据统计报告等。

- 报表内容:包括多数据库综合分析、性能状态、会话分布、语句分布、风险分析等。
- 统计图展现形式:包括饼状图、柱形图、条形图、双轴折线图等。
- 报表样例:例如,日报中的数据库访问压力统计报告,如图 12-233:数据库访问压力统计报告所示。

图 12-233: 数据库访问压力统计报告



- 3. 导出报表或为当前报表设置定时推送。
 - 单击导出,选择导出格式,单击确定,可导出当前报表。

说明: 报表支持以Word、PDF、HTML格式导出。

单击加入定时推送任务,选择推送任务,填写报表名称,选择报表格式,单击确定,可为当前报表设置定时推送。

12.4.3.3.2 管理定时推送任务

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到报表页面,单击定时推送,管理定时推送任务。

单击新增,在新增任务组对话框中,输入任务名称、邮件主题,设置发送周期、发送时间,勾选需要发送的用户,单击保存,可新增定时推送任务组,如图 12-234:新增定时推送任务组所示。

图 12-234: 新增定时推送任务组

云盾•数据库审计		🕰 概况 💷	1 报表 💙 配置	▶维	沪				≤ (0) 🛓 secadmin 👻 😁 退
日报周报月报。	萨班斯报告 PCI排	资产端风险分析	客户端工具应用分析报	浩 审计记录	数统	计报告 定时	推送		
	邮件主题	新増任务组							操作
	tsett		114.000		444.544	-10-201	40.00	n	▲ ■ 2 8 ■
缺省周发送任务	定时发送报表	任务名称	11方百杯		友达	失型 secadmin	即相 td@db.com		8 🗆 🖉 e 📾
缺省日发送任务	定时发送报表	邮件主题	邮件主题			sysadmin	lidekui@dbsec.com		
缺省月发送任务	定时发送报表	发送周期	天			sysauditor			
		发送时间	请填写0~23时点						
		启用	启用 ▼						
									•
							保存	取消	

- 选择任务列表中的任务,单击右侧操作栏中的编辑按钮,可修改该任务组的相关参数,并可 启用或禁用该任务组。
- 选择任务列表中的任务,单击右侧操作栏中的删除按钮,单击确定,可删除该任务组。
- 选择任务列表中的任务,单击右侧操作栏中的任务列表按钮,可查看该任务组中的报表定时 推送任务,并且通过单击编辑和删除按钮,可以修改该任务的报告格式及任务名称,或删除 该推送任务。
- 选择任务列表中的任务,单击右侧操作栏中的发送历史按钮,可查看该任务组已发送报表的 历史记录。

12.4.3.4 系统告警信息

云盾数据库审计系统具备系统监控能力,支持通过系统内告警信息的方式提示安全管理员系统异常 情况。

12.4.3.4.1 查看系统告警信息

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 单击页面右上角的系统告警按钮,打开**系统告警信息**对话框,如图 12-235: 查看系统告警信息所示。

图 12-235: 查看系统告警信息

	▲ 概況 ▲ 风		句 🗩 会话			を配置			2) 🛔 secadmin	▼ ● 退出
sqiserver ・ 政策部ド(1) 三元全部・ 前代考末 ・ 10 ・ 764,252 月出告書 64,653 64,653 64,653 64,653 61,653 61,653 61,653		系統告留信息 告留关型 全部	8 ▼	'æ: ह ▼)	确认状态: 未确认 ▼	所号 没生时间 1 2018-01-08 15:57 2 2018-01-08 15:32	石登二世 7:18 Agent异常 3:15 Agent异常	v 加入5	97#1865\$ I	
			3 风险分 3.1 风J 注: 纪)布状况 俭命中统计 计时间内,被零	甲计数据库产业的风	から水水に、年め月ナガブドネボ 当時間形金均踏无政策	(截拼斥的风险状态	关闭		Ţ

3. 选择告警类型、恢复状态、确认状态,单击查询,可查看指定类型或状态的告警信息。

送 说明:	
在描述栏中可查看该告警信息的具体触发原因。	

4. 检查并处理该系统异常后,单击操作栏中的确认按钮,该信息将不再告警。

12.4.3.4.2 配置系统告警

背景信息

系统告警信息也支持通过邮件方式进行通知,便于相关管理人员及时了解系统异常。

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到配置页面,单击系统告警设置,如图 12-236:系统告警设置所示。

图 12-236: 系统告警设置

云盾•数据库管	制计		🕰 概況	🛄 报表 🛛 📽 🕅	置 ト 维护			🛥 (0) 🗳 secadmin ◄	🕒 退出
系统告警设置	授权管理	IP名称管	理						
☑邮件通知			用户名称	角色		邮件地址	用户状态	通知	Î
			sysauditor	系统审	+员		启用		
			sysadmin	系统管	記	lidekui@dbsec.com	启用		
			secadmin	安全管	題员	td@db.com	启用		
		由区	件标题						
		3	发生时间 风险级别	告警类型 告警描述					
									1
		4						Þ	×
		告	警周期 1	(分钟)				
									定

3. 勾选需要通过邮件通知的管理人员。

修改管理人员的邮件地址,需使用管理员账号登录后,单击右上角的账户名,在下拉菜单中选择**用户资料**,在**用户资料**对话框中即可进行修改。

4. 填写邮件标题,在文本框中输入邮件内容。

单击文本框上方的发生时间、风险级别、告警类型、告警描述,可将这些变量信息添加至邮件 内容中。

5. 填写最短告警周期,即最短多少分钟内发送一次系统告警邮件通知,单击确定。

12.4.3.5 配置

配置页面主要用于云盾数据库审计系统的告警信息配置及授权管理配置,包含系统告警设置、授权管理、IP名称管理等。

12.4.3.5.1 授权管理

在授权管理页面,安全管理员可进行用户管理及功能授权,如图 12-237:授权管理页面所示。

图 12-237: 授权管理页面

	云盾•数据	库审计	🔒 概況	山报表	\$ 配置	▶ 维护				≤(0) Lescadmin - () 退出
2	《统告警设置	授权管理	IP名称管理							
	用户名	角色名称	用户有效期	邮件地址	手机号码	启用		操作	数据库	
	sysadmin	系统管理员	2099-12-31 21:16:13	lidekui@dbsec.com	139020254	96 💌	Ø	ê		权限
	sysauditor	系统审计员	2099-12-31 21:16:13				Ø	1	数据库测试	● 只读 ○ 读写
	secadmin	安全管理员	2099-12-31 21:16:13	td@db.com	139020254	95 💌	Ø	ê	菜单	
								● 添加用户	 ● 全庫 維护 ● 全庫 総元 ● 全庫 総元 ● 単庫 総元 ● 単庫 260 ● 単庫 265 ● 単庫 記量 	劉儀柱

12.4.3.5.1.1 用户管理

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到配置页面,单击授权管理,管理数据库审计系统用户,如图 12-238: 用户管理所示。

☐ 说明:

默认的系统管理员、系统审计员、安全管理员无法修改或删除。

图 12-238: 用户管理

用户名	角色名称	用户有效期	邮件地址	手机号码	启用		操作
sysadmin	系统管理员	2099-12-31 21:16:13	Reiningsbeec.com	13902025496	•	Ø	۵
sysauditor	系统审计员	2099-12-31 21:16:13			•	3	
secadmin	安全管理员	2099-12-31 21:16:13	td@db.com	13902025495		3	<u>ل</u>
testtest	系统操作员	2018-01-22 14:34:34	test@3.com	12467788645		Ø	ش
							四 添加用户

- 单击添加用户,在添加用户对话框中,设置用户信息(其中,用户名、密码、用户有效期为 必填项),单击保存,即添加新用户。
- 在用户列表中,选择用户,勾选或取消启用,可设置是否启用该用户。
- 在用户列表中,选择用户,单击修改按钮,可修改该用户的信息。
- 在用户列表中,选择用户,单击删除按钮,单击确定,可删除该用户。

12.4.3.5.1.2 功能授权

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到**配置**页面,单击**授权管理**,选择已启用的用户,为该用户进行授权,如图 *12-239*:功能授权所示。

送明:

默认的系统管理员、系统审计员、安全管理员的权限无法修改。

图 12-239: 功能授权



• 数据库权限:勾选需要授权给该用户的数据库,并选择只读或读写权限。

- 菜单权限:勾选需要授权给该用户的功能节点
- 3. 单击保存,单击确定。

12.4.3.5.2 IP名称管理

背景信息

IP名称管理主要用于实现IP业务化,将IP地址与具有业务含义的IP名称关联,便于云盾数据库审计系统的用户理解某些IP地址的业务含义。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到配置页面,单击IP名称管理,如图 12-240: IP名称管理所示。

图 12-240: IP名称管理

云盾•数据库审计	88 概况	■ 报表 🗳 配置	▶ 维护		👅 (0) 🛔 seca	dmin 👻 🕩 退出
系統告警设置 授权管理	IP名称管理					
IP地址	» IP段 IP名称	变更时间	-			Q查询
IP业务化列表					◎ 导入 ◎	导出 🔡 添加
检索条件为:无						
序号 IP地址			IP名	33	变更时间 操作	

- 单击添加,在添加业务化IP对话框中,输入IP地址或IP段,及对应的IP名称,单击确定,即可添加IP名称记录。
- 单击导入,选择格式规范的CSV文件,单击确定,可批量导入业务化IP信息。



在**导入业务化数据**对话框中,单击**请先下载IP业务化文件模板**,可下载标准格式模板。

- 单击导出,可将当前IP业务化列表以CSV格式导出至本地。
- 在IP业务化列表上方,设置IP地址或IP段、IP名称、变更时间查询条件,单击**查询**,可查看相应的IP业务化记录。

12.4.3.6 维护

维护页面用于对审计系统本身业务安全与稳定性进行保障维护。数据库审计系统是以审计日志及日 志存储文件为基础。因此,如何妥善存储、备份、整理审计日志是本系统确保安全的关键。

维护页面包含数据备份恢复、Agent管理、恢复出厂设置、引擎管理四大功能模块。

12.4.3.6.1 数据备份恢复

本系统基于审计日志的安全性和永久性考虑,进行常规的审计日志的备份操作。通过对审计日志进行定制的备份存储,减少系统存储压力。同时,通过便捷的日志恢复功能,随时对备份数据进行查询与恢复。

数据备份恢复页面分为上下两栏,包括备份机制和备份清单查询。

本系统支持自动备份与手动备份两种备份方式:

- 自动备份:备份审计日志
- 手动备份:备份系统配置数据

12.4.3.6.1.1 设置自动备份

操作步骤

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击数据备份恢复。
- 3. 在自动备份配置区域,设置开始备份时间、备份内容,选择是否将备份上传FTP服务器,如图 12-241:设置自动备份所示。

图 12-241: 设置自动备份

自动备份配置 备份 3 ▼ 天前数据 开始备份时间 1 ▼ 点 □]保存 □ FTP设置 ?	
---	--

- **开始备份时间**:自动备份以天为单位,通过开始备份时间确定在哪一整点时间开始每天的自动备份。
- 备份内容:自动备份默认备份3天前的数据,即备份自当天起三天前的数据。例如,在12月17日,自动备份默认备份12月14日当天的审计日志数据。
- FTP设置: 启用后,系统根据分区空间自动向FTP服务器的指定路径上传审计日志。
- 4. 单击保存。

12.4.3.6.1.2 手动备份与恢复

- 1. 使用安全管理员(secadmin)账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击数据备份恢复。

3. 在手动备份/恢复区域,单击备份,如图 12-242: 手动备份所示。

图 12-242: 手动备份

手动备份/恢复 备份 O	恢复 🛛	

4. 单击确定,对当前系统配置数据进行备份。

备份成功后,在手动备份/恢复区域,单击**恢复**,选择备份文件,单击**确认**,即将该备份的系统 配置数据恢复并覆盖当前系统配置数据,如图 12-243: 手动恢复所示。

图 12-243: 手动恢复

手动恢复	
	浏览
请慎重使用:会覆盖当前系统配置!	
	确认取消

12.4.3.6.1.3 查询备份清单

背景信息

自动备份的数据默认会存储到数据库审计系统的硬盘,也可以选择上传到FTP服务器转存。安全管 理员可在备份清单表中查看备份执行记录。

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击数据备份恢复。
- 3. 设置查询日期,默认查询条件以月为单位,统计某月内的备份记录。
- 4. 选择数据状态,可选择的数据状态包括:
 - 全部:本系统审计到的全部数据查询。
 - 在线:本系统中未被清理、恢复,并且在线可查询的初始数据。
 - 已恢复:本系统中清理后被恢复的数据。
 - 已清理:本系统中达到系统阈值被清理的数据。
 - 处理中:本系统当前正在进行清理或者恢复的数据。

5. 单击**查询**或刷新,查看相应的备份记录。备份清单列表包含备份日期、数据状态、备份结果、FTP上传状态、空间占用等信息。

📕 **说明**:

如果自动备份启用FTP设置,且备份已成功转存至FTP服务器,在操作栏中单击恢复,可将该日 志备份恢复至数据库审计系统硬盘。

12.4.3.6.2 Agent管理

Agent管理主要包含Agent下载、Agent配置部署等功能。

12.4.3.6.2.1 下载Agent

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击Agent管理。
- 3. 单击下载Agent, 如图 12-244: 下载Agent所示。

图 12-244: 下载Agent

④ | 下载Agent [下载Agent] 下载需要部署到被保护数据库服务器上的Agent程序

- 4. 单击确定,打开Agent部署配置对话框。
- 5. 将已下载的Agent程序上传并安装至需要被审计的数据库服务器。
- 6. 在Agent部署配置对话框中,输入数据库所在服务器的IP地址,单击添加。

在IP地址栏中输入多个IP地址(每个IP地址一行),单击**添加**,可批量添加服务器IP地址。

📔 说明:

请务必完成Agent部署配置。如未配置,Agent程序抓取的数据将无法被审计。

部署配置完成后,云盾数据库审计系统即可对该数据库进行审计。

12.4.3.6.2.2 Agent自动部署

背景信息



建议多应用环境的服务器使用该功能部署Agent,只支持Linux系统。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击Agent管理。
- 3. 单击Agent自动部署,打开Agent自动部署对话框,如图 12-245: Agent自动部署所示。

图 12-245: Agent自动部署

Anent自动部	『署	
Agent配置: □本地回环 (●审计服务器	(应用程序与数据库在同一台机器上) 滑IP:	
目标服务器:	192.168.100.88,pwd,22 192.168.100.89,pwd,22 格式:目标IP,root密码,ssh端	
	「「「」「」「」「」「」「」「」」「」「」」「」」「」」「」」「」」「」」「」	取消

根据实际情况勾选是否本地回环(应用程序与数据库在同一台机器上),输入云盾数据库审计系统服务器IP及目标服务器信息,单击部署。

	送明:
	目标服务器信息格式为:目标服务器IP,root密码,ssh端口
5.	开始部署后,单击 查看执行日志 ,可查看自动部署执行情况。

等待部署完成,目标服务器会自动下载并安装Agent。Agent安装完成后,需要前往**Agent部署配 置**对话框中完成Agent部署配置。

12.4.3.6.3 恢复出厂设置

背景信息

本系统出于安全性考虑,提供恢复出厂设置功能。

- 清理审计数据:删除系统下所有的审计日志,仅保留所有的策略和配置数据。
- 恢复出厂设置:删除系统下所有的业务数据(审计日志、配置数据等)以及配置数据,恢复至出 厂状态配置。

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击恢复出厂设置,如图 12-246:恢复出厂设置所示。

图 12-246: 恢复出厂设置



- 3. 根据需要,执行恢复出厂设置操作。
 - 单击清理审计数据。
 - 单击恢复出厂设置。
- 4. 单击确定。

12.4.3.6.4 引擎管理

操作步骤

- 1. 使用安全管理员 (secadmin) 账号登录云盾数据库审计系统。
- 2. 定位到维护页面,单击引擎管理,如图 12-247:引擎管理所示。
 - 图 12-247: 引擎管理

性值 ▼ ▼	单位	描述 這择ms npchtwinpls的模式,0 npcintwinpls(正常版本默认),1 rms (云版本默认),2 (共存模式)	
性值 ▼ ▼	单位	描述 涟缩rms npc/nfw/npls的模式,0 npc/nfw/npls(正常版本默认),1 rms (云版本默认),2 (共存模式)	
T		选择rms npc/nfw/npls的模式,0 npc/nfw/npls(正常版本默认),1 rms (云版本默认),2 (共存模式)	
Υ 			
•		审计选项,可以选择全部审计或者满足审计规则审计	
		结果集审计开关	
	Kb	结果集最大保存长度,范围是1~64k,确保整行显示,默认为1k	
	行	结果集最多保存行数,范围是1~999	
٣	条	实例下,每天最多记录的告警次数	
		NPP进程池参数,0 表示不开启进程池;大于0 表示开启进程池,并代表进程池中NPP进程的数量;默认为0,范围:0-8000	
•		默认值为1(通用型)或2(MSSOL型),默认为1	
¥		支持sqlserver2005/2008用户名解析开关,默认0关闭,开启为1	
Ŧ		当发生TCP超时流量放行,1-开启,0-关闭,默认关闭	
•		安全实例自动重启开关,默认为开启	
	秒	系统监控进程的监控时间间隔	
	秒	系统监控进程的检查其他进程是否工作的时间间隔	
	秒	系统监控进程的检查其他进程是否存活的时间间隔	
	秒	后台TLW进程刷新TLOG缓冲区的的最长时间间隔(如果TLOG缓)中区的数据不足2M的情况下),范围:3-3600	
	¥ ¥ ¥	マ マ マ マ マ マ マ ひ む む む む	17 14年来県を14715AL 2014度 1999 S 案例下、毎天最多は3分前2番次数 NPP担握協参案、0表示不开出注理治:大子0表示开出注理治:井代表注理治:中NPP进程的数量: 飲认为0, 范围: 0-8000 取以值为1 (通用型) 或2 (MSSQL型), 飲认为1 文持5glserve20052008用产名條所开关, 飲认以次辺, 开启为1 世发生TCP超初活量软行, 計20.头因, 就认决辺 安全条件同 3週世界大, 軟认为开启 彩 系统监控进程的监控时间间隔 彩 系统监控进程的监控时间间隔 彩 系统监控进程的监控时间间隔 彩 系统监控进程的监控时间间隔

证书状态 正常 系统时间: 2018-01-11 09:44:32

- 单击启动或停止,可启动或停止数据库审计引擎。
- 单击刷新,刷新引擎的当前状态及配置信息。
- 在常用配置区域,设置引擎的配置属性值,单击保存,修改引擎配置。



单击**恢复默认值**,可将配置属性恢复至默认值。

12.4.4 审计管理员指南

审计管理员与系统管理员(sysadmin)和安全管理员(secadmin)不同,其主要职责是通过查看系统审计日志对云盾数据库审计系统本身进行审计管理。

12.4.4.1 查看系统操作日志

操作步骤

- 1. 使用审计管理员 (sysauditor) 账号登录云盾数据库审计系统。
- 在审计日志页面,选择数据库,选择查询时间范围,单击查询,查看数据库审计系统操作日志,如图 12-248: 审计日志所示。



单击条件,可针对用户、登录IP、动作等信息设置更精准的查询条件。

图 12-248: 审计日志

云盾•贺踞库申讨 日志 S(1) ≜ sysauditor →	🕩 退出									
<u>审计日志</u>										
数 週席 所有 マ 0 今天 昨天 本周 上周 本月 上月 自定义 マ 条件	Q查询									
	*									
序号 用户 登录IPA 发生时间 功能 动作 数据库 描述 结果	€ľF									
1 sysauditor 10.36.1.129 2018-01-11 11:23:51 暨录 登录 用户登录: sysauditor 成功	•									
2 sysauditor 10.36.1.129 2018-01-11 11:21:09 登录 登录 用户登录: sysauditor 失败										
	#26									

单击日志记录列表右上角的导出报告按钮,选择**csv导出**,可将当前列表中的审计日志记录导出 到本地。

 选择审计日志记录,单击操作栏中的详细按钮,可以查看该审计日志的详细信息,如图 12-249: 审计日志详细信息所示。

单击操作栏中的删除按钮,可以删除该日志记录。另外,单击日志记录列表上方的清空日志记录 按钮,可删除所有日志记录。

图 12-249: 审计日志详细信息



12.5 数据发现与脱敏

12.5.1 登录专有云数据安全控制台

专有云数据安全控制台面向专有云平台租户开放,可供租户为自己部门中的数据库进行数据抽取、 数据脱敏和数据隐藏等的数据处理操作。

前提条件

确认您所使用的账号已具备相应部门的云资源权限,例如具备部门管理员角色权限。

- 1. 登录云盾安全中心。
- 定位到数据安全 > 数据发现与脱敏,单击DDM,如图 12-250: 登录数据发现与脱敏控制台所示。

图 12-250: 登录数据发现与脱敏控制台



12.5.2 专有云数据安全控制台界面

专有云数据安全控制台的界面主要分为三大区域,功能菜单、数据统计、任务信息,如图 12-251: 专有云数据安全控制台界面所示。



图 12-251: 专有云数据安全控制台界面

各区域详细说明如表 12-10: 专有云数据安全控制台区域说明所示。

表 12-10: 专有云数据安全控制台区域说明

区域	说明
功能菜单	单击不同的功能菜单时,将进入相应功能的界面。
数据统计	展示已发现的敏感数据的统计和分布信息。
任务信息	展示最近发生的数据发现及脱敏任务数据。

12.5.3 使用指南

12.5.3.1 数据源管理

登录专有云数据安全控制台之后,您可以连接生产数据库、文件源等数据源,并对数据源进行管理。

12.5.3.1.1 数据库

12.5.3.1.1.1 添加数据库

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据源管理 > 数据库列表页面,单击添加数据库,如图 12-252: 数据库列表页面所示。

图 12-252: 数据库列表页面

数服	数据库列表 [31:00095 第99									
数据	裤名称	: 数据库名称	IP地址:	IP地址	授業					
	序号	數据库名称	数据库类型	IP地址	端口	数据库名	实例名	创建用户	时间	操作
	1	mysql-rds2	MySql	80.004/WT/000	3306	test2		22222222	2017-10-30 17:55:38	Q (2 8
8	2	mysql-rds	MySql	6008.01199	3306	test1		22222222	2017-10-30 17:55:00	Q (7 8
	3	ADS2	ADS	where the the tobaco.	10047	adstest2		22222222	2017-10-25 10:29:03	Q (7 8
8	4	ADS1	ADS	alkinst Tilliki Icco	10035	adstest		22222222	2017-10-25 10:28:05	Q (8 8
	5	odps数据库2	ODPS	http://www.odps.ali	0		dbsec2	22222222	2017-10-24 11:04:03	Q (7 8
	6	Odps数据库	ODPS	importantion relps.ali	0		dbsec	22222222	2017-10-24 11:01:49	Q (7 8

3. 在**添加数据库**对话框中,输入数据库名称,选择数据库类型,输入数据库地址、数据库端口、数 据库名、用户名、密码、描述等信息,如图 12-253: 添加数据库所示。

图 12-253: 添加数据库

	◎ 添加数据库	×
数据库名称	测试数据库	
数据库类型	MySql •	
数据库地址	47	
数据库端口	9207	
数据库名	datashield	
用户名	root	
密码	•	
描述	描述	
	//////////////////////////////////////	
测试连接		保存取消

4. 单击测试连接。

如果测试连接失败,请检查输入的数据库信息是否正确,建议仅在测试连接成功时保存数据库信息。

5. 连接测试成功后,单击保存,即完成数据库的添加。

说明:

- 数据库名称不允许重复。
- 数据库信息记录不允许重复。
- 对于Oracle类型的数据库,通过"数据库主机IP+数据库主机端口+数据库实例名"的方式 确定唯一的数据库信息记录。

12.5.3.1.1.2 修改数据库

操作步骤

1. 登录专有云数据安全控制台。

- 定位到数据源管理 > 数据库列表页面,选择需要修改的数据库信息记录,单击右侧的编辑按钮,如图 12-254:编辑数据库所示。
 - 图 12-254: 编辑数据库

 序号<数据集支控</th>
 数据集支控
 IP地位
 第二
 数据集客
 实明名
 使理用户
 對面
 操作

 1
 mysql-rds2
 Mysql
 mail
 3306
 text2
 2222222
 2017-10-30 175538
 0 7
 8

3. 在编辑数据库对话框中,修改数据库信息,单击保存。



12.5.3.1.1.3 删除数据库

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据源管理 > 数据库列表页面,选择需要删除的数据库信息记录,单击右侧的删除按钮,如图 12-255: 删除数据库所示。
 - 图 12-255: 删除数据库

序号	数据库名称	数据库类型	IP地址	端口	数据库名	实例名	创建用户	时间	操作
1	mysql-rds2	MySql	10.000 million	3306	test2		22222222	2017-10-30 17:55:38	Q 🕼 🔒

3. 在信息提示对话框中,单击确定,删除该数据库信息记录,如图 12-256:确认删除提示所示。

图 12-256: 确认删除提示

● 信息提注	× z
您确定删除吗?	
	确定取消

n un		
	1×100.	
	1. 况明 .	

删除数据库信息记录时,如果该数据库信息与专有云数据安全系统内其他数据存在关联,将无法删除该数据库信息记录,如图 12-257: 删除数据库信息提示所示。这种情况下,您需要先完成该数据库关联信息的清理,才可删除该数据库信息记录。

图 12-257: 删除数据库信息提示

● 信息提示	×
此数据库已关联以下信息,不能进行删除操作!	
发现任务1个: odps-zljtm001	
方案1个: odps-zljtm001	
实体1个: odps-zljtm001	
	确认

12.5.3.1.1.4 查询数据库

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据源管理 > 数据库列表页面,输入数据库名称或IP地址,单击搜索,如图 12-258:搜索 数据库信息记录所示,即可查询包含所输入信息的数据库信息记录。

📕 说明:

数据库搜索功能支持模糊查询。

图 12-258: 搜索数据库信息记录

数据库名称: 数据库名称 IP地址: IP地址	搜索	
-------------------------	----	--

3. 选择数据库信息记录,单击右侧的查看按钮,可查看该数据库的详细信息,如图 12-259: 查看数 据库所示。

图 12-259: 查看数据库

Q 查看数据库			
数据库名称	mysql-rds2		
数据库类型	MySqI		
数据库地址	60(205)117:149		
数据库端口	3306		
数据库名	test2		
描述	描述		

12.5.3.1.2 文件源

专有云数据安全支持将数据库导出的数据文件作为数据源进行脱敏处理,支持csv和txt格式的平面 文件。

从数据库导出的平面文件相当于一张数据库表,若干个平面文件的集合则相当于一个数据库。因此,专有云数据安全定义了**文件源**的概念,在同一个文件源中的平面文件,具有相同的存储位置和 管理方式,且这些文件内部具有逻辑关系。

12.5.3.1.2.1 添加文件源

操作步骤

1. 登录专有云数据安全控制台。

2. 定位到数据源管理 > 文件源列表页面,单击添加,如图 12-260:文件源列表页面所示。

图 12-260: 文件源列表页面

文件 文件	源列表 源名称	: 文件源名称 按 宏			添加 删除 配置
	序号	文件源名称	描述	修改时间	操作
	1	zljtm002.txt		2017-11-08 14:20:45	■ Q Ø ≘
	2	zljtm001自定义.txt		2017-10-26 14:42:03	∎ Q Ø 8
	3	zljtm001.txt		2017-10-26 09:35:13	■ Q Ø ⊜

3. 在添加文件源对话框中,输入文件源名称、描述,单击保存,如图 12-261: 添加文件源所示。

图 12-261: 添加文件源

	● 添加文件源	×
文件源名称	用户手册演示	
描述	用于演示如何创建文件源	
~		保存取消
☐ 说明:		

文件源名称不允许重复。

12.5.3.1.2.2 添加文件

- 1. 登录专有云数据安全控制台。
- 定位到数据源管理 > 文件源列表页面,选择文件源信息记录,单击右侧的文件列表按钮,如图 12-262:打开文件列表所示。

图 12-262: 打开文件列表

序号	文件源名称	描述	修改时间	操作
1	test		2017-12-07 15:22:39	₽ Q Ø @
2	zljtm002.txt		2017-11-08 14:20:45	■ Q Ø 8

3. 在文件列表对话框中,单击添加,如图 12-263: 文件列表对话框所示。

图 12-263: 文件列表对话框

		■ 文件列表		×
				添加
序号	文件名称	字符集	修改时间	操作
1	zljtm002.txt	UTF-8	2017-11-08 14:21:06	Q 🕼 🔒
₩ « 1	» N Go a	页 5 🔻 条 共1条		
				关闭

- 4. 在添加文件对话框中,单击选择文件,选择一个数据文件。
- 选择该文件的字符集、行分隔符、列包围符、列分隔符、日期格式、日期分隔符、时间分隔符、 小数点符、日期时间排序、是否有表头,单击保存,如图 12-264:添加文件所示,将该文件添加 到文件源中。

图 12-264: 添加文件

	● 添加文件	>
文件源名称	zljtm002.txt	
文件名称	Choose File No file chosen	
选择文件模板	默认不使用模板 ▼	
是否带表头	不带表头	
字符集	UTF8	
行分隔符	CRLF (Windows) • 自定义	
列分隔符	逗号(,) • 自定义	
列包围符	双引号(") ▼ 自定义	
日期样例:	2017/12/07 15:54:17	
日期时间排序	日期时间	
		保存 取消
说明:		

- 添加文件时,文件源名称无法修改。
- 同一文件源中,无法添加重复文件。

12.5.3.1.2.3 修改文件

- 1. 登录专有云数据安全控制台。
- 2. 定位到**数据源管理 > 文件源列表**页面,选择文件源信息记录,单击右侧的文件列表按钮。
- 3. 在文件列表对话框中,选择已添加的文件,单击右侧的编辑按钮,如图 12-265: 文件列表所示。

图 12-265: 文件列表

		■ 文件列表		>
				添加
序号	文件名称	字符集	修改时间	操作
1	zljtm002.txt	UTF-8	2017-11-08 14:21:06	Q 🕜 🔒
K ≪ 1	» N	Go 每页 5 T 条 共1条		
				关闭

4. 在编辑文件对话框中,修改该文件的相关设置信息,单击保存,如图 12-266:编辑文件所示。

图 12-266: 编辑文件

	☞ 编辑文件	-	
文件源名称	zljtm002.txt		
文件名称	zljtm002.txt	¥	
选择文件模板	默认不使用模板	T	
是否带表头	不带表头	T	
字符集	UTF8	T	
行分隔符	CRLF (Windows) •	自定义	
列分隔符	逗号(,) 🔹	自定义	
列包围符	无	自定义	
日期样例:	2017-12-07 16:01:48		
日期时间排序	日期时间	T	
		保存	取

在编辑文件对话框中,文件源名称及文件名称无法修改。

12.5.3.1.2.4 删除文件

前提条件

删除文件前,请确认该文件与专有云数据安全系统中其它数据已无关联。

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据源管理 > 文件源列表页面,选择文件源信息记录,单击右侧的文件列表按钮。
- 3. 在**文件列表**对话框中,选择已添加的文件,单击右侧的删除按钮,如图 12-267: 文件列表所示。

图 12-267: 文件列表

		■ 文件列表		
				添加
序号	文件名称	字符集	修改时间	操作
1	zljtm002.txt	UTF-8	2017-11-08 14:21:06	Q 🖉 🔒
K « 1	» H 📃 🖸	0 每页 5 ▼ 条 共1条		
				关闭

4. 在信息提示对话框中,单击确定,如图 12-268: 删除文件提示所示,删除该文件。

图 12-268: 删除文件提示

● 信息提示	×
您确定删除吗?	
确定	取消

12.5.3.1.2.5 修改文件源

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据源管理 > 文件源列表页面,选择文件源信息记录,单击右侧的编辑文件源按钮,如图 12-269:文件源列表所示。

图 12-269: 文件源列表

序号	文件源名称	描述	修改时间	操作
1	test		2017-12-07 15:22:39	b Q 🕼 8
2	zljtm002.txt		2017-11-08 14:20:45	₽ Q Ø 8

3. 在编辑文件源对话框中,修改文件源描述,如图 12-270:编辑文件源所示。

图 12-270: 编辑文件源

	✓ 编辑文件源	×
文件源名称	用户手册演示	
描述	用于演示如何创建文件源	
		保存取消



文件源名称无法修改。

12.5.3.1.2.6 删除文件源

前提条件

删除文件源前,请确认该文件源记录与专有云数据安全系统内其他数据已无关联。

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据源管理 > 文件源列表页面,选择文件源信息记录,单击右侧的删除文件源按钮,如图 12-271:文件源列表所示。

图 12-271: 文件源列表

序号	文件源名称	描述	修改时间	操作
1	test		2017-12-07 15:22:39	S Q 🖉 🔒
2	zljtm002.txt		2017-11-08 14:20:45	■ Q Ø 8

3. 在信息提示对话框中,单击确定,如图 12-272: 删除文件源提示所示,删除该文件源。

图 12-272: 删除文件源提示

● 信息提示	×
忽确定删除吗?	
	确定 取消

12.5.3.1.2.7 查询文件源

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据源管理 > 文件源列表页面,输入文件源名称,单击搜索,如图 12-273: 搜索文件源所 示,即可查询包含所输入信息的文件源信息记录。

道 说明 : 文件源搜索功能支	持模糊查询。		
图 12-273: 搜索文	件源		
文件源名称:	文件源名称	搜索	

3. 选择文件源信息记录,单击右侧的查看按钮,如图 12-274: 查看文件源所示,可查看该文件源的 详细信息。

图 12-274: 查看文件源

序号	文件源名称	描述	修改时间	操作
1	test		2017-12-07 15:22:39	₽ Q Ø 8
2	zljtm002.txt		2017-11-08 14:20:45	₽ Q 27 8

12.5.3.2 数据发现

专有云数据安全支持按照所选的发现规则,对数据库和文件源中的数据库表和文件进行敏感数据识

别,并展示识别结果。

12.5.3.2.1 发现任务

12.5.3.2.1.1 数据库发现任务

12.5.3.2.1.1.1 添加数据库发现任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 发现任务页面,单击添加,如图 12-275:发现任务列表所示。

图 12-275: 发现任务列表

发现任 纪 运行物	客列表 【态: 全部运行状态	▼ 发现任	务名称: 发现任务名称	数据源	3称: 数据源名称		搜索 下级		添加
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	-
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	

3. 在添加发现任务对话框的基本信息页签中,输入任务名称,选择数据库任务类型,选择数据 库,单击下一步,如图 12-276: 添加发现任务基本信息页签所示。

图 12-276: 添加发现任务基本信息页签

		Э 添加发现任务 ×
基本信息 数据配置 规	则配置 采样配置	
任約	务名称任务名称	
任約	务类型数据库	Ŧ
数	据库 test1	Ŧ
		下一步 关闭
说明:		

任务名称不可重复。

- 4. 在**添加发现任务**对话框的**数据配置**页签中,输入用户名、密码,单击连接。
- 5. 测试连接成功后,在右侧显示的模式及数据库表信息中,勾选您想要执行发现任务的数据库 表,单击**下一步**,如图 *12-277:* 添加发现任务数据配置页签所示。

图 12-277: 添加发现任务数据配置页签

基本信息 数据配置 规则配置 采样配置		
当前选择的数据源:test	数据源浏览(1)	
用户名 root	模式名称全部	▼表名称
密码・	□ 序号 模式名称	表名称
许接	20 test2	sm_check_log
连接成功!	21 test2	sm_check_method
	✓ 22 test2	systemuser
	23 test2	test
	24 test3	systemuser
	25 test3	systemuser2
	№ « 13 14 15	» ▶ Go 每页 30 ▼条 共445条

- 6. 在**规则配置**页签中,选择发现规则,单击**下一步**,如图 *12-278:* 添加发现任务规则配置页签所示。
 - 图 12-278: 添加发现任务规则配置页签

		J				
置发现规则:						□ 全)
✔ Email地址	✔ 中文地址	✔ 中文姓名	✔ 企业名称组织机构	× 其他	✔ 姓名和单位名称	
× 座机号码	✔ 手机号码	✔ 日期	× 纳税人识别号	× 统一社会信用代码	✔ 证件号	
✔ 身份证号	× 金額数字	✔ 银行卡号				
定义发现规则:						□ 全)
× 111111	× 1212	× 666	× test001	× 产品代码	× 海关编号	
× 经营单位	× 证券内码					
	配置组合发现规则					
配置: □ @						
处配置: □ 4						
处配置: □ □						

送 说明:

关于发现规则的具体介绍参见发现规则。

7. 在采样配置页签中,设置采样规则,单击保存,如图 *12-279*: 添加发现任务采样配置页签所示,即可完成数据库发现任务的添加。

图 12-279: 添加发现任务采样配置页签

				● 添加发现任务	×
基本信息	数据配置	规则配置 采	羊配置		
采样规则:				采样抽取说明:	
采样前	1000	行进行分	析	1、抽取前m行进行分析,系统先抽取连续m行分析 不够m行的,抽取全部数据进行分析。 2 第m行之后的数据抽取n%-进行分析	
抽取数据的	1	‰进行分	析	3、抽取前m行,从m+1行开始采样率为千分之n, 最多采样50万行。	
				上一步 保存 保存并运行 关键	đ

采样规则举例:

- 假设数据库表中有10000行数据,采样前1000行,再抽取数据的1‰进行分析,则一共会抽取1000+(10000-1000)*1‰=1009行数据根据发现规则进行数据发现。
- 假设数据库表中有800行数据,采样前1000行,再抽取数据的1‰进行分析,则一共会抽取 800行数据进行发现规则验证。

12.5.3.2.1.1.2 执行数据库发现任务

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已添加的数据库发现任务,单击任务记录右侧的操作列表,单击运行任务,如图 12-280:发现任务列表所示。
图 12-280: 发现任务列表

发现任务 运行状	务列表 术态: 全部运行状态	▼ 发现(1务名称: 发现任务名称	数据	源名称 : 数据源名称		搜索 下载		添加
序号	发现任务名称	任务类型	數据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	=
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:4	▶运行任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	自制除任务
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49		☞ 編輯任务
7	mysol-parts	教福室	mysal-rds	100%	完成.	2222222	2017-11-01 17:23:14	2017-10-31 09:58:54	■ 历史任务

3. 在运行发现任务对话框中,输入用户名、密码,选择是否启用发现关系,单击检测,如图 12-281: 运行发现任务所示。



启用发现关系后,在运行数据库发现任务时可发现数据库中数据表之间的关系。关于数据关系 发现的具体介绍参见数据关系。

图 12-281: 运行发现任务

	▶ 运行发现任务		×
数据源			
数据库	mysql-rds		
用户名	请输入正确的用户名]	
密码	请输入正确的密码]	
发现关系	禁用 启用		
		检测 取消	当

4. 检测通过后,单击运行,该数据库发现任务即开始执行。

等待数据库发现任务执行完毕,如图 12-282:数据库发现任务执行完成所示。

图 12-282: 数据库发现任务执行完成

 序号
 发展任务名称
 任务类型
 数据原第
 任务进度
 运行状态
 深加用户
 深加时间
 上次完成时间
 操作

 1
 test
 数据序
 test
 100%
 光成
 test,ccg
 2017/09/04 06:59:58
 2017/09/04 07:00:35
 雪

12.5.3.2.1.1.3 停止数据库发现任务

背景信息

当数据库发现任务运行时,可以参考以下操作步骤停止该发现任务:

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择正在执行的数据库发现任务,单击任务记录右侧的操作列表,单击停止任务,如图 12-283:发现任务列表所示,即可终止正在执行的发现任务。

图 12-283: 发现任务列表

运行物	《态: 全部运行状态	• 2	友现任务名称: 发现任务名称	数据》	除名称: 数据源名称		搜索 下载			
序号	发现任务名称	任务类型	數据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作	
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12		
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	=	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48		
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	▶运行任务	
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	■ 19止115 自制除任务	
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49		☞ 编辑任务	
7	mysol-parts	約据库	mysal-rds	100%	金成	22222222	2017-11-01 17:23:14	2017-10-21 09-58-54	■ 历史任务	

12.5.3.2.1.1.4 查看数据库发现任务的历史记录

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已执行的数据库发现任务,单击任务记录右侧的操作列表,单击历史任务,如图 12-284:发现任务列表所示。

图 12-284: 发现任务列表

发现任务列表											
运行	式态: 全部运行状态	▼ 发现(任务名称: 发现任务名称		数据源名称: 数据源名称		搜索 下载				
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作		
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	=		
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38			
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48			
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	▶ 运行任务		
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	● 制除任务		
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49		☞ 编辑任务		
7	mysol-parts	教程度	mysal-rds	100%	宗成	22222222	2017-11-01 17:23:14	2017-10-31 09:58:54	回历史任务		

3. 在**发现任务执行记录**对话框中,选择任务记录,单击右侧的执行报告按钮,如图 *12-285*: 发现任务执行记录所示。

图 12-285: 发现任务执行记录

			☰ 发现任务执行记录			×
② 量近一周	服近一个月 木月 上月 自定文					按索
任务号	任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作
327	100%	完成	test_ccg	2017-09-04 07:00:33	2017-09-04 07:00:35	
326	100%	完成	test_ccg	2017-09-04 07:00:21	2017-09-04 07:00:23	B 0
325	100%	完成	test_ccg	2017-09-04 07:00:09	2017-09-04 07:00:11	• •
324	100%	完成	test_ccg	2017-09-04 06:58:01	2017-09-04 06:58:02	. 0
323	100%	完成	test_ccg	2017-09-04 06:57:51	2017-09-04 06:57:51	• •
322	100%	完成	test_ccg	2017-09-04 06:57:40	2017-09-04 06:57:41	
321	100%	灾成	test_ccg	2017-09-04 06:57:28	2017-09-04 06:57:29	• •
N « 1 »)	₩ 60 每页 30 ▼条 共8条	et ult		0017 00 04 00 57 05	0017 00 04 00 57 05	• •
						关闭

4. 在**发现任务执行报告**页面中,查看该发现任务的执行信息,如图 *12-286:*发现任务执行报告所示。

图 12-286: 发现任务执行报告

发现任务执行报告									
基本信息									
任务名称: test				任务运行时间]: 2秒5毫秒				
任务总对象数(表/文件):	32			发现敏感对象	改(表/文件): 7				
任务总列数(字段/文件列)	: 276			发现敏感列数	な(字段/文件列): 13				
发现任务执行信息									
执行信息列表							执行		
运行状态: 全部运行状	太・「「横式名」	描述夕	丰夕.	主々	地志				
EIIWA: EPEIIW	况, (天八石.	快以口	1211.	48.11	12.34				
□ 序号 数据源	模式	表	运行状态	总列数	敏感列数	总行数	发现行数		
🔲 1 test	datashield	datadiscoveryrule	完成	17	1	35	35		
2 test	sonar	project_qprofiles	完成	3	0	0	0		
🔲 3 test	sonar	properties	完成	8	0	6	6		
🔲 4 test	sonar	qprofile_changes	完成	6	0	1001	1000		
□ 5 test K « 1 2 » M	sonar Go 每页 30 ▼	quality_gates 条 共32条	完成	4	1	1	1		
异常日志列表									
日志级别:全部	▼ 错误名:	结误名	表名·	事么	油卖				
		икч		1214	76.21				
序号 错误名称	严重级	别表名	任务号	任务类别 错	误详细信息		时间		
		无	数据						
K « 1 » X 🗌 G	● 每页 30 ▼ 条	共0条							

5. 在**发现任务执行记录**对话框中,选择任务记录,单击右侧的下载执行日志按钮,如图 *12-287*: 下载执行日志所示,可将该发现任务的执行日志下载到本地。

图 12-287: 下载执行日志

			☰ 发现任务执行证	示录		×
 ● 単近一月 	最近一个月 本月 上月 自定文					按索
任务等	子 任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作
327	100%	完成	test_ccg	2017-09-04 07:00:33	2017-09-04 07:00:35	N (0)
326	100%	完成	test_ccg	2017-09-04 07:00:21	2017-09-04 07:00:23	B (0)
325	100%	完成	test_ccg	2017-09-04 07:00:09	2017-09-04 07:00:11	 0
324	100%	完成	test_ccg	2017-09-04 06:58:01	2017-09-04 06:58:02	b 0
323	100%	完成	test_ccg	2017-09-04 06:57:51	2017-09-04 06:57:51	 0
322	100%	完成	test_ccg	2017-09-04 06:57:40	2017-09-04 06:57:41	
321	100%	完成	test_ccg	2017-09-04 06:57:28	2017-09-04 06:57:29	 0
N « 1	» N Go 每页 30 ▼条 共8条	171-8		0017 00 04 00 57 05	0017 00 04 00 57 05	F (1)
						关闭

12.5.3.2.1.1.5 编辑数据库发现任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已添加的数据库发现任务,单击任务记录右侧的操作列表,单击编辑任务,如图 12-288:发现任务列表所示。

图 12-288: 发现任务列表

发现任务 运行状	3列表 法态: 全部运行状态	▼ 发现日	务名称: 发现任务名称	数据	苦源名称: 数据源名称		搜索 下载		添加
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	=
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	▶ 运行任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	自制除任务
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49	[☞ 編輯任务
7	mysol-parts	数据库	mysal-rds	100%	完成	2222222	2017-11-01 17:23:14	2017-10-31 09:58:54	■ 历史任务

3. 在编辑发现任务对话框中,可变更需要被发现的数据库表、发现规则、采样规则,修改完成 后,单击保存,如图 12-289:编辑发现任务所示。

图 12-289: 编辑发现任务

			✔ 编辑发现任务	
基本信息	数据配置	規则配置	采样配置	
		15 12 12 200	test	
		在另右怀	lest	
		任务类型	数据库 ▼	
		数据库	test •	
			下一步	X

任务名称、任务类型、和数据库无法修改。

12.5.3.2.1.1.6 查看数据库发现任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 发现任务页面,选择已添加的数据库发现任务,单击任务发现名称。
- 3. 在发现任务详情页面,查看该数据库发现任务的详细信息,如图 12-290: 发现任务详情页面所示。

图 12-290: 发现任务详情页面

发现任务i	洋情								
基本信息 任务名称: 任务类型:	test 数据库发现任务	创 建 者: 连续抽取:	test_ccg 1000 (行)	创建时间: 抽样比例:	2017-09-04 06:59:58 1 ‰				
配置的数据 数据源类型	源信息 : 数据库	数据源名称:	test						
已配置的数	据源列表								
schema名称 table名称 sonar project_qprofiles properties qprofile_changes quality_gate_conditions quality_gates resource_index rule_repositories rules rules_parameters rules_profiles schema_migrations snapshots user_roles user_tokens users webhook_deliveries									
test	active_rule_parameters duplications_index	active_rules events file_sour	authors ce_activity ces group_roles g	ce_queue ce_s proups groups_use	scanner_context ce_task_inp rs internal_properties	ut			
test2	systemuser								
datashield	datadiscoveryrule								
規則配置信息 已配置的发现规则: 多份证号 银行卡号 手机号码 中文姓名 中文地址 证件号 企业名称组织机构 姓名和单位名称 日期 Email地址 已配置的组合发现规则:									
序号	组合发现规则名称			发现规则名称					
			无数据						

12.5.3.2.1.1.7 删除数据库发现任务

前提条件

删除数据库发现任务前,请确认该发现任务与专有云数据安全系统中其它数据已无关联。

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已添加的数据库发现任务,单击任务记录右侧的操作列表,单击删除任务,如图 12-291:发现任务列表所示。

图 12-291: 发现任务列表

发现任 美	务列表 式态: 全部运行状态	▼ 发现(迁务名称: 发现任务名称	数	据源名称 : 数据源名称		搜索 下载		添加
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	=
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	▶ 运行任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	自制除任务
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49		☞ 编辑任务
7	mysol-parts	教捐產	mysal-rds	100%	完成	22222222	2017-11-01 17:23:14	2017-10-31 09:58:54	画 历史任务

3. 在信息提示对话框中,单击确定,删除该数据库发现任务。

12.5.3.2.1.2 文件发现任务

12.5.3.2.1.2.1 添加文件发现任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 发现任务页面,单击添加,如图 12-292:发现任务列表所示。

图 12-292: 发现任务列表

发现任 约	客列表 《态: 全部运行状态	▼ 发现日	1务名称: 发现任务名称	数据源谷	3称: 数据源名称		搜索 下载		添加
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	

3. 在添加发现任务对话框的基本信息页签中,输入任务名称,选择文件任务类型,选择文件源,单击下一步,如图 12-293: 添加发现任务基本信息页签所示。

图 12-293: 添加发现任务基本信息页签

	● 添加发现任务 ×								
基本信息 数据配置 規則配置 采相	基本信息 数据配置 规则配置 采样配置								
任务名称	任务名称								
任务类型	文件								
文件源	test •								
	下一変大切	J							
~									
送 说明:									

任务名称不可重复。

4. 在添加发现任务对话框的数据配置页签中,勾选您想要执行发现任务的文件,单击**下一步**,如图 12-294: 添加发现任务数据配置页签所示。

图 12-294: 添加发现任务数据配置页签

2			(▶ 添加发现任	务			×
基本信息	数据配置	规则配置	采样配置					
当前选择的文	件源: test							
文件名称:	文件名称		搜索					
□ 序号	文件名称							
1	test.csv							
						上一步	下一步	闭

5. 在规则配置页签中,选择发现规则,单击**下一步**,如图 *12-295*: 添加发现任务规则配置页签所示。

图 12-295: 添加发现任务规则配置页签

- 6. 在**采样配置**页签中,设置采样规则,单击**保存**,如图 *12-296*: 添加发现任务采样配置页签所 示,即可完成文件发现任务的添加。
 - 图 12-296: 添加发现任务采样配置页签

基本信息 数据配置 规则配置 采样加取 采样前 1000 行进行分析 1. 抽取前師行进行分析,系统先抽取连续m行分析, 不够而行め,抽取全部数据进行分析。 油取数据的 1 %。进行分析 1. 抽取前師行,从m+1行开始采样率为千分之n, 最多采样50万行。					● 添加发现任务	×
采样規則: 采样抽取说明: 采样前 1000 行进行分析 抽取数据的 1 %进行分析 1 %进行分析 3、抽取前师行,从m+1行开始采样率为千分之n, 最多采样50万行。	基本信息	数据配置	规则配置	采样配置		
采样前 1000 行进行分析 1、抽取前加行进行分析,系统先抽取连续加行分析。 不够加行的,抽取全部数据进行分析。 油取数据的 1 %。进行分析 3、抽取前加行,从m+1行开始采样率为千分之n, 最多采样50万行。	采样规则:				采样抽取说明:	
抽取数据的 1 %。进行分析 3、抽取前m行,从m+1行开始采样率为千分之n, 最多采样50万行。 上一步 保存 保存并运行 关闭	采样前	1000	行进	行分析	1、抽取前m行进行分析,系统先抽取连续m行分析 不够m行的,抽取全部数据进行分析。 2、第m行之后的数据抽取n‰进行分析。	
上一步 保存 保存并运行 关闭	抽取数据的	1	‰进	行分析	3、抽取前m行,从m+1行开始采样率为千分之n, 最多采样50万行。	
上一步 保存 保存并运行 关闭						
上一步 保存 保存并运行 关闭						
上一步 保存 保存并运行 关闭						
上一步 保存 保存并运行 关闭						
					上一步 保存 保存并运行 关门	团



关于发现规则的具体介绍参见发现规则。

采样规则举例:

- 假设数据库表中有10000行数据,采样前1000行,再抽取数据的1‰进行分析,则一共会抽取1000+(10000-1000)*1‰=1009行数据根据发现规则进行数据发现。
- 假设数据库表中有800行数据,采样前1000行,再抽取数据的1‰进行分析,则一共会抽取 800行数据进行发现规则验证。

12.5.3.2.1.2.2 执行文件发现任务

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已添加的文件发现任务,单击任务记录右侧的操作列表,单击运行任务,如图 12-297:发现任务列表所示。

图 12-297: 发现任务列表

发现任约	客列表								添加
运行划	法 全部运行状态	* 3	发现任务名称: 发现任务名称	数据	源名称: 数据源名称		搜索 下戰		
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	▶ 运行任务
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	●停止任务 會删除任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	☞ 编辑任务
6	assault	数据应	mysal-rds	0%	未执行	2222222	2017-10-31 10:30:49		■ 历史任务

3. 在运行发现任务对话框中,单击检测,如图 12-298:运行发现任务所示。

图 12-298: 运行发现任务

	▶ 运行发现任务	×
检测列表		
1.文件是否存在		
		检测 取消

4. 检测通过后,单击运行,该文件发现任务即开始执行。

12.5.3.2.1.2.3 停止文件发现任务

背景信息

当文件发现任务运行时,可以参考以下操作步骤停止该发现任务:

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择正在执行的文件发现任务,单击任务记录右侧的操作列表,单击停止任务,如图 12-299:停止文件发现任务所示,即可终止正在执行的发现任务。

图 12-299: 停止文件发现任务

发现任命	客列表								添加
运行物	t态: 全部运行状态	▼ 发现任	E务名称: 发现任务名称	数据》	原名称: 数据源名称		搜索 下载		
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	▶ 运行任务
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	自删除任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	☞ 編輯任务
6	assault	教棋座	mysal-rds	0%	未执行	2222222	2017-10-31 10:30:49		画 历史任务

12.5.3.2.1.2.4 查看文件发现任务的历史记录

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已执行的文件发现任务,单击任务记录右侧的操作列表,单击历史任务,如图 12-300:发现任务列表所示。

图 12-300: 发现任务列表

发现	现任务列	列表									添加
ìž	行状态	5: 全部运行状态	▼ 发现任	务名称: 发现任务名称		数据源名称:	数据源名称		搜索 下载		
鸤	号 2	发现任务名称	任务类型	数据源	任务进展	r.	运行状态	添加用户	添加时间	上次完成时间	操作
	1 0	odps-jctm001	数据库(ODPS)	Odps数据库	100%		完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	
	2 z	ljtm002.txt	文件	zljtm002.txt	100%		完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	=
	з г	ds-tm	数据库	mysql-rds	100%		完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	▶ 运行任务
	4 0	DDPS2-zljtm001	数据库(ODPS)	odps数据库2	100%		完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	■ 特止性务 自删除任务
	5 c	odps-zljtm002	数据库(ODPS)	Odps数据库	100%		完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	G2 编辑任务
	6 a	issault	教掘座	mysal-rds	0%		未执行	222222	2017-10-31 10:30:49		■ 历史任务

3. 在**发现任务执行记录**对话框中,选择任务记录,单击右侧的执行报告按钮,如图 *12-301:* 发现任务执行记录所示。

图 12-301: 发现任务执行记录

			〓 发现任务执行记录			×
0 8 2- A	医一个月 本月 上月 自定文					
任务号	任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作
322	100%	完成	test_ccg	2017-09-07 15:26:51	2017-09-07 15:26:51	
H « 1 » H	▲ 単页 30 ● 崇 共1条					
						关闭

4. 在发现任务执行报告页面中,查看该发现任务的执行信息,如图 12-302: 发现任务执行报告所示。

图 12-302: 发现任务执行报告

又现任务执行报告							
基本信息							
壬务名称: test			任务运行时	1间: 51毫秒			
任务总对象数(表/文件):	: 1		发现敏感对象数(表/文件): 0				
任务总列数(字段/文件列)):1		发现敏感列	数(字段/文件列)	: 0		
发现任务执行信息							
执行信息列表						执行	
运行状态: 全部运行	状态 ▼ 文件名:	表名	搜索				
□ 序号 文件源	文件	运行状态	总列数	敏感列数	总行数	发现行数	
l test	test.csv	完成	1	0	1	1	
K 《 1 》 X 📃 🕻 당승미主제主	60 每页 30 ▼条 共1	Â					
K ≪ 1 ≫)	Go 毎页 30 ▼ 条 共1: ▼ 错误名: :	条 错误名	文件名 : 文件名	授援	Ŕ		
K ≪ 1 ≫ K ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Go 每页 30 ▼ 条 共1: ▼ 错误名: 严重级别	条 错误名 文件名	文件名: 文件名 任务号 任务类别	援援	Ŕ	时间	
№ 《 1 》) 【 ♀常日志列表 日志级别: 全部 序号 错误名称	Go 每页 30 ▼ 条 共1 ▼ 错误名: 2 严重级别	条 错误名 文件名 无数3	文件名: 文件名 任务号 任务类别	接送详细信息	ŝ	时间	
 N 《 1 》 N 《 4 P常日志列表 日志级别: 全部 序号 错误名称 	Go 每页 30 ▼ 条 共1: ▼ 错误名: 严重级别	条 错误名 文件名 无数据	文件名: 文件名 任务号 任务类别	接到	R	时间	
 № (1 »)) ▶) ♀常日志列表 日志级别: 全部 序号 错误名称 	Go 每页 30 ▼条共1 ▼ 错误名: 严重级别	条 错误名 文件名 无数	文件名: 文件名 任务号 任务类别	接送详细信息	Ŕ	时间	
 K 《 1 》) F常日志列表 日志级别: 全部 序号 错误名称 	Go 每页 30 ▼ 条 共1: ▼ 错误名: 严重级别	条 错误名 文件名 无数据	文件名: 文件名 任务号 任务类别	接到	R	时间	
 N (1)) (1)) (1))) (1)))))	Go 每页 30 ▼条共1 ▼ 错误名: 严重级别	条 错误名 文件名 无数 *	文件名: 文件名 任务号 任务类别	接到	6	时间	

5. 在**发现任务执行记录**对话框中,选择任务记录,单击右侧的下载执行日志按钮,如图 *12-303*: 下 载执行日志所示,可将该发现任务的执行日志下载到本地。

图 12-303: 下载执行日志

			■ 发现任务执行记录			×
0 MX-R	最近一个月 末月 上月 自定文					
任务号	任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作
322	100%	完成	test_ccg	2017-09-07 15:26:51	2017-09-07 15:26:51	
N « 1	◎ M [] 10 10 10 10 新井1条					
						关闭

12.5.3.2.1.2.5 编辑文件发现任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已添加的文件发现任务,单击任务记录右侧的操作列表,单击编辑任务,如图 12-304:发现任务列表所示。

图 12-304: 发现任务列表

发现任	务列表								添加
运行	状态: 全部运行状态	* *	过现任务名称: 发现任务名称	数	居源名称 : 数据源名称		搜索 下载		
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	=
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	▶ 运行任务
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	● 停止性务 自 删除任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	☞ 编辑任务
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49		□ 历史任务

3. 在编辑发现任务对话框中,可变更需要被发现的文件、发现规则、采样规则,修改完成后,单击保存,如图 12-305:编辑发现任务所示。

图 12-305: 编辑发现任务

	● 编辑发现任务 ×
基本信息 数据配置 规则配置	采样配置
任务名称	test
任务类型	文件
文件源	test •
	下一步 关闭
~	
送明 :	

任务名称、任务类型、和文件源无法修改。

12.5.3.2.1.2.6 查看文件发现任务

操作步骤

1. 登录专有云数据安全控制台。

- 2. 定位到数据发现 > 发现任务页面,选择已添加的文件发现任务,单击任务发现名称。
- 3. 在发现任务详情页面,查看该文件发现任务的详细信息,如图 12-306: 发现任务详情页面所示。

图 12-306: 发现任务详情页面

发现任务详	情					
基本信息 任务名称: 任务类型:	test 文件发现任务	创 建 者: 连续抽取:	test_ccg 1000 (行)	创建时间: 抽样比例:	2017-09-07 15:24:50 1 ‰	
配置的数据源 数据源类型:	原信息 文件源	数据源名称:	test			
已配置的数据 文件源名称 test	苦源列表 文件名称 test.csv					
规则配置信息 已配置的发现 身份证号 已配置的组合	8. 印规则: 银行卡号 手机号码 中文姓 含发现规则:	名 中文地址 证	E件号 日期 Ema	ill地址		
序号	组合发现规则名称			发现规则名称		
			无数	据		

12.5.3.2.1.2.7 删除文件发现任务

前提条件

删除文件发现任务前,请确认该发现任务与专有云数据安全系统中其它数据已无关联。

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择已添加的文件发现任务,单击任务记录右侧的操作列表,单击删除任务,如图 12-307: 删除发现任务所示。
 - 图 12-307: 删除发现任务

发现任务	务列表								添加
运行状	太 态: 全部运行状态	Ŧ	发现任务名称: 发现任务名称	数	据源名称: 数据源名称		搜索 下载		
序号	发现任务名称	任务类型	数据源	任务进度	运行状态	添加用户	添加时间	上次完成时间	操作
1	odps-jctm001	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-08 14:45:32	2017-11-08 14:46:12	
2	zljtm002.txt	文件	zljtm002.txt	100%	完成	22222222	2017-11-08 14:21:34	2017-11-08 14:21:38	
3	rds-tm	数据库	mysql-rds	100%	完成	22222222	2017-11-08 14:16:36	2017-11-08 14:16:48	▶ 运行任务
4	ODPS2-zljtm001	数据库(ODPS)	odps数据库2	100%	完成	22222222	2017-11-08 14:11:53	2017-11-08 14:12:45	自制除任务
5	odps-zljtm002	数据库(ODPS)	Odps数据库	100%	完成	22222222	2017-11-06 10:45:38	2017-11-06 10:46:18	⑦ 编辑任务
6	assault	数据库	mysql-rds	0%	未执行	22222222	2017-10-31 10:30:49		■ 历史任务

3. 在信息提示对话框中,单击确定,删除该文件发现任务。

12.5.3.2.1.3 查询发现任务

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现任务页面,选择运行状态,输入发现任务名称,单击搜索,如图 12-308:
 查询发现任务所示,查询包含所设定条件的发现任务。

图 12-308: 查询发现任务

运行状态:	全部运行状态	发现任务名称:	发现任务名称	数据源名称:	数据源名称	搜索 📩

12.5.3.2.2 敏感字段梳理

执行数据库发现任务后,专有云数据安全系统会将数据库表所有的字段和匹配的敏感数据发现规则等信息展示在敏感字段梳理页面。

12.5.3.2.2.1 添加敏感数据源

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 敏感字段梳理页面,在数据源列表区域,单击添加,如图 12-309:数据源列表所示。

图 12-309: 数据源列表



- 3. 在新增敏感数据对话框中,选择数据源,输入用户名、密码,单击连接,如图 12-310: 新增敏感数据所示。
 - 图 12-310: 新增敏感数据

			● 添加敏感数据	×
选择数据源			数据源浏览(0)	
数据源	test	Ŧ	模式名称 全部 ▼ 表名称 表名称	
用户名	root		□ 序号 模式名称 表名称	
密码	•		📄 🖬 1 datashield algorithm	
连接			C datashield algorithm_mix	
连接成功!			E 3 datashield audit_log	
			📄 🖬 4 datashield codetoken	
			E 5 datashield databasediscoverytask	
			E 6 datashield databaseinfo	
			K 《 1 2 3 4 5 6 ») Go 每页 30 ▼条 共445	条
			保存	关闭



连接成功后,数据源浏览区域会显示数据库表名称及模式名称。

 勾选需要被发现的数据库表,单击保存,新增的敏感字段将显示在敏感字段梳理页面的敏感数据 列表中。

12.5.3.2.2.2 核实敏感数据

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 敏感字段梳理页面,在敏感数据列表区域,核实已发现的敏感数据字段。
 - 选择敏感数据记录,单击右侧的核实此敏感数据按钮,如图 12-311:核实敏感数据记录所示,核实该敏感数据。

图 12-311: 核实敏感数据记录

●敏感数据	洌表 ≁ 🗹			□ 未核	实字段 🛛 已	核实字段 🛛	敏感数据字段	□ 变更字段	□ 按时间倒	序 ✔展开更	多条件 土	ba:	下载
序号	状态	模式	表	字段	字段备注	发现规则	敏感级别	样本	数据类型	约束类型	是否核实	操作	
1		dbsec	jctm001	email地址		Emailte v	低	gong_1043	STRING		未核实	۶	
2		dbsec	jctm001	money		金額数字 🔻	低	-121.33	DOUBLE(0,0)		未核实	18	
3		dbsec	jctm001	中文地址		中文地址 🔻	高	上海市海淀	STRING		未核实	1 1	

单击敏感数据列表区域上方的核实当前页按钮,如图 12-312:核实当前页敏感数据记录所示,核实当前页面所有敏感数据记录。

图 12-312: 核实当前页敏感数据记录

● 敏感数据列	列表 ♪ 🗹]		■ 未核	实字段 🛛 已	核实字段 🔲	敏感数据字段	} □ 变更字段	□ 按时间倒	序 →展开更	多条件 投	数 下载
序号	状态	模式	表	字段	字段备注	发现规则	敏感级别	样本	数据类型	约束类型	是否核实	操作
1		dbsec	jctm001	email地址		Email地 v	低	gong_1043	STRING		未核实	18
2		dbsec	jctm001	money		金额数字 🔻	低	-121.33	DOUBLE(0,0)		未核实	18
3		dbsec	jctm001	中文地址		中文地址 🔻	高	上海市海淀	STRING		束核实	18
4		dbsec	jctm001	中文姓名		中文姓名 🔻	高	张三丰	STRING		未核实	18
5		dbsec	jctm001	企业名称组		企业名称 🔻	ф	湖南京剧艺	STRING		未核实	18
6		dbsec	jctm001	座机号码		非敏感数 🔻	非敏感	010236525	STRING		未核实	18
7		dbsec	jctm001	手机号码		手机号码 🔻	高	+86186235	STRING		未核实	18

12.5.3.2.2.3 设置为非敏感数据

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 敏感字段梳理页面,在敏感数据列表区域,选择已发现的敏感数据记录,单击 右侧的设置为非敏感数据按钮,如图 12-313:设置为非敏感数据所示。

在敏感级别栏中已标识为非敏感的数据记录无法设置为非敏感数据。

图 12-313: 设置为非敏感数据

序号	状态	模式	表	字段	字段备注	发现规则	敏感级别	样本	数据类型	约束类型	是否核实	操作
1		dbsec	jctm001	email地址		非敏感数 🔻	非敏感	gong_1043	STRING		已核实	⊁ ⊗
2		dbsec	jctm001	money		金額数字 🔻	低	-121.33	DOUBLE(0,0)		未核实	1 3
3		dbsec	jctm001	中文地址		中文地址 🔻	高	上海市海淀	STRING		未核实	1

3. 在信息提示对话框中,单击是,如图 12-314: 设置非敏感数据信息提示所示。

图 12-314: 设置非敏感数据信息提示

♀ 信息提示	×
设置为非敏感数据可能影响有关方案的配置,是否继续?	
是	否

▋ 说明:

设置为非敏感数据的数据记录的敏感级别将变成非敏感,其发现规则也将变更为非敏感数据。

12.5.3.2.2.4 修正敏感数据

背景信息

数据库发现任务可以多次执行,当第一次发现任务的结果被人为修改或者被发现的数据库表发生变 化时,第二次发现任务的结果可能和第一次的不同。这种情况下,需要安全管理人员修正敏感数 据。

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 敏感字段梳理页面,在敏感数据列表区域,选择状态为新增、已变更或已删
 除的敏感数据记录,单击右侧的修正此敏感数据按钮,如图 12-315: 敏感数据列表所示。

图 12-315: 敏感数据列表

敏感数据	洌表											
≈ ≓	۶ 🖉			□ 未核	这字段 ■ 日	核实字段 🗌	敏感数据字段	段 🔲 变更字段	2 🗌 按时间的	到序 マ展开 !	更多条件	搜索 下载
序号	状态	模式	表	字段	字段备注	发现规则	敏感级别	样本	數据类型	约束类型	是否核实	操作
1		adstest	zljtm001	addr		中文地址 •	高	内蒙古呼和	varchar		已核实	⊁ ⊗
2	=	adstest	zljtm001	date		日期 •	低	2005/11/02	date		朱核实	F 8 8
3		adstest	zljtm001	email		Emailted v	低	Aa23bb@s	varchar		已核实	F ®
4	≓	adstest	zljtm001	money		金额数字 🔻	低	122.23	float		未核实	F 8 8
5		adstest	zljtm001	name		中文姓名 🔻	高	李洪武	varchar		已核实	F ®
6		adstest	zljtm001	nsmum		傍税人诉 🔻	高	110108685	varchar		已核实	18

- 3. 在修正敏感数据对话框中,修正该敏感数据记录,如图 12-316:修正敏感数据所示。
 - 单击修正,新发现的敏感数据将会覆盖原敏感数据记录。
 - 单击保留、或关闭,放弃本次修正操作。

图 12-316: 修正敏感数据

				🖋 修正敏	感数据				
★ 修正操作会	。将新发现的铜	放感数据覆盖到	医原敏感数据						
	模式	表	字段	字段备注	发现规则	样本	数据类型	数据长度	刻度
原敏感数据	datashield	datadiscov	defaultalg…	默认脱敏算…	手机号码	1	int	11	0
新发现敏感数据	datashield	datadiscov	defaultalg…	默认脱敏算…		1	int	11	0
								保留	修正关键

12.5.3.2.2.5 查询敏感数据

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 敏感字段梳理页面,单击展开更多条件,如图 12-317: 搜索敏感数据记录所

示。

- 输入模式、表名、字段名、字段备注等信息,单击搜索,查询包含所设定条件的敏感数据记录。
- •选择发现规则,单击搜索,查询相应发现规则的发现的敏感数据。
- 选择显示未核实字段、显示敏感数据字段、当前变更字段,单击搜索,显示相应敏感数据。

图 12-317: 搜索敏感数据记录

≍ ≓	F I	□ 末核3	实字段 📄 已核实字段 📄 敏感数据字段 📄 支更字段 📄	抜时间倒序 へ 取縮更多条件 捜索 📩
发现规则:	全部規則			
模 式:	模式	表 名:	表名	
字段名:	字段名	字段备注:	字段备注	

12.5.3.2.3 敏感文件梳理

执行文件发现任务后,专有云数据安全系统会将文件源中所有的字段和匹配的敏感数据发现规则等 信息展示在**敏感文件梳理**页面。

12.5.3.2.3.1 核实敏感数据

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据发现 > 敏感文件梳理页面,在敏感文件列表区域,核实已发现的敏感数据字段。
 - 选择敏感数据记录,单击右侧的核实此敏感数据按钮,如图 12-318:核实敏感数据记录所示,核实该敏感数据。

图 12-318: 核实敏感数据记录

敏感文件	列表						
∞ ≓	۶ 🖌		🛛 未核实字段 🗎	已核实字段 🔲 敏感数据字段 🛙	◎ 变更字段 🔲 按时间倒序	▼ 展开更多条件	搜索 下载
序号	状态	文件名	列序号 列标题	发现规则	样本	是否核实	操作
1		zljtm001.txt	1	金额数字 ▼	-121.33	已核实	18
2	≓	zljtm001.txt	2	纳税人识别号	13010519770501123401	未核实	<u> </u>
3		zljtm001.txt	3	非敏感数据	4869444488887777027	已核实	18
4		zljtm001.txt	4	手机号码 🔻	+8618623536985	已核实	18
5	≓	zljtm001.txt	5	座机号码 ▼	01023652521	未核实	⊁ ⊗ ⊗
6		zljtm001.txt	6	中文姓名	张三丰	已核实	18

单击敏感文件列表区域上方的核实当前页按钮,如图 12-319:核实当前页敏感数据记录所示,核实当前页面所有敏感数据记录。

图 12-319: 核实当前页敏感数据记录

敏感文件 → → →	·列表		□ 未核实字段 □	■已核实字段 ■ 敏感数据字段 ■	变更字段 🗌 按时间倒序	▼展开更多条件	搜索 下载
序号	状态	文件名	列序号 列标题	发现规则	样本	是否核实	操作
1		zljtm001.txt	1	金额数字 ▼	-121.33	已核实	18
2	≓	zljtm001.txt	2	纳税人识别号 ▼	13010519770501123401	未核实	188
3		zljtm001.txt	3	非敏感数据	4869444488887777027	已核实	18
4		zljtm001.txt	4	手机号码 🔻	+8618623536985	已核实	18
5	≓	zljtm001.txt	5	産机号码・・	01023652521	未核实	188
6		zljtm001.txt	6	中文姓名	张三丰	已核实	18

12.5.3.2.3.2 设置为非敏感数据

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 敏感文件梳理页面,在敏感文件列表区域,选择已发现的敏感数据记录,单击 右侧的设置为非敏感数据按钮,如图 12-320:设置为非敏感数据所示。



在敏感级别栏中已标识为非敏感的数据记录无法设置为非敏感数据。

图 12-320: 设置为非敏感数据

序号	状态	文件名	列序号 列标题	发现规则	样本	是否核实	操作
1		zljtm001.txt	1	金額数字 🔻	-121.33	已核实	×
2	≓	zljtm001.txt	2	纳税人识别号 ▼	13010519770501123401	未核实	188
3		zljtm001.txt	3	非敏感数据	4869444488887777027	已核实	18

3. 在信息提示对话框中,单击是,如图 12-321: 设置为非敏感数据信息提示所示。

图 12-321: 设置为非敏感数据信息提示



说明:

设置为非敏感数据的数据记录的敏感级别将变成非敏感,其发现规则也将变更为非敏感数据。

12.5.3.2.3.3 修正敏感数据

背景信息

文件发现任务可以多次执行,当第一次发现任务的结果被人为修改或者被发现的文件发生变化

时,第二次发现任务的结果可能和第一次的不同。这种情况下,需要安全管理人员修正敏感数据。

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 敏感文件梳理页面,在敏感文件列表区域,选择状态为新增、已变更或已删
 除的敏感数据记录,单击右侧的修正此敏感数据按钮,如图 12-322: 敏感文件列表所示。

图 12-322: 敏感文件列表

敏感文件	列表						
≍ ≓	۶ 🖌		□ 未核实字段 □	已核实字段 💷 敏感数据字段 🛙	〕 变更字段 🔲 按时间倒的	▶ ▶ 展开更多条件	搜索 下载
序号	状态	文件名	列序号 列标题	发现规则	样本	是否核实	操作
1		zljtm001.txt	1	金額数字 ▼	-121.33	已核实	18
2	=	zljtm001.txt	2	纳税人识别号 🔻	13010519770501123401	未核实	₽ 8 8
3		zljtm001.txt	3	非敏感数据	486944488887777027	已核实	18
4		zljtm001.txt	4	手机号码 🔻	+8618623536985	已核实	18
5	≓	zljtm001.txt	5	產机帶码 ▼	01023652521	未核实	188
6		zljtm001.txt	6	中文姓名	张三丰	已核实	18

- 3. 在修正敏感数据对话框中,修正该敏感数据记录,如图 12-323:修正敏感数据所示。
 - 单击修正,新发现的敏感数据将会覆盖原敏感数据记录。
 - 单击保留或关闭,放弃本次修正操作。

图 12-323: 修正敏感数据

			🖋 修正敏感数	据			
★ 修正操作会将新发现的敏感数据覆盖至原敏感数据							
	文件名称	列序号	列标题	发现规则	样本	数据长度	
原敏感数据	testFile.csv	1		纳税人识别号	1111111111111111	73	
新发现敏感数据	testFile.csv	1		其他	1111111111111111	73	
					_		
					6	溜 修正 关	J

12.5.3.2.3.4 查询敏感数据

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 敏感文件梳理页面,单击展开更多条件,如图 12-324: 搜索敏感数据记录所示。
 - 输入文件名,单击搜索,查询包含所设定条件的敏感数据记录。
 - 选择发现规则,单击搜索,查询相应发现规则的发现的敏感数据。
 - 选择显示未核实字段、显示敏感数据字段、当前变更字段,单击搜索,显示相应敏感数据。

图 12-324: 搜索敏感数据记录

敏感文件列表	
$x \rightleftharpoons \not > \boxtimes$	□ 未核实字段 □ 已核实字段 □ 敏感数据字段 □ 变更字段 □ 按时间倒序 ▲ 收益更多条件 搜索 下载
发现规则: 全部规则	▼ 文件名: 文件名

12.5.3.2.4 发现规则

专有云数据安全系统内置了15种发现规则,用于发现用户数据中的敏感数据。

12.5.3.2.4.1 查看发现规则

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现规则页面,在发现规则列表区域选择发现规则记录,右侧的规则基本信息
 区域将展示该发现规则的规则信息,如图 12-325: 查看发现规则所示。
 - 添加 发现规则列表 规则基本信息 规则名称: 身份证号 规则描述 发现身份证号(18个数字字符,最后一个 规则名称 T Q 字符会存在X) 发现方式: * 按正则发现 测试样本: 样本数据 ▼ 内置规则 敏感等级 敏感-高 ۳ 确认比例: 身份证号 统一社会信用代码 正则表达式: (^\d{6}((((19|20)\d{2}))(0[13-9]|1[012])(0[1-9]| 姓名和单位名称 纳税人识别号 推荐脱敏算法信息 日期 1.身份证号楷换 2.身份证号随机 3.证件号楷换(含身份证、军官证、港澳通行证等) 4.证件号随机(含身份证、军官证、港澳通行证等) 预判断信息 Email地址 根行卡号 序号 特征类别 特征项 **最小值(起始位) 最大値(结束位)** 手机号码 任意字符 15 15 1 字符数量规则 座机号码 字符数量规则 任意字符 18 18 2 中文姓名 字符数量规则 数字 15 15 3 中文地址 数字 17 17 4 字符数量规则 证件号 字符数量规则 数字 18 18 5 企业名称组织机构 字符数星相同
 - 图 12-325: 查看发现规则

3. 在规则基本信息区域的**测试样本**框中,输入测试数据,单击**测试**可对发现规则进行测试。 符合该发现规则的数据,提示通过;不符合的测试数据,则提示不通过。

12.5.3.2.4.2 添加自定义发现规则

- 1. 登录专有云数据安全控制台。
- 定位到数据发现 > 发现规则页面,可以在发现规则列表区域单击添加,并在规则基本信息区域设置自定义规则的相关信息,单击保存,如图 12-326:添加发现规则所示。

图 12-326: 添加发现规则

发现规则列表	规则基本信息			保存
规则名称 ▼ Q	规则名称: 发现规则名称		规则描述: 描述	
	发现方式: 按正则发现	Ŧ		k
▼ 内置规则	敏感等级 敏感-高	¥	测试样本: 样本数据	368%
身份证号	确认比例: 匹配率	%		
统一社会信用代码	正则表达式: 正则表达式			
姓名和单位名称		ĥ		
纳税人识别号	高级设置			
日期	预判断设置 推荐脱敏算法			
Email地址	kamistani			
银行卡号	和四天空: 字符数量规则	*		
手机号码	序号 特征项	最小数量	最大数量	操作
座机号码				+

12.5.3.3 数据脱敏

专有云数据安全为了便于对数据库表的数据进行抽取,定义了"数据子集"的概念。通过定义数据 子集,您可以对符合一定条件的数据进行脱敏。

12.5.3.3.1 数据子集

12.5.3.3.1.1 添加数据子集

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 数据子集页面,单击左侧数据子集区域的添加,如图 12-327:数据子集列表所示。

图 12-327: 数据子集列表

数据子集列表	添加 删除
数据子集名称	T Q
□ 全选	
🔲 test	6
rds-tm	6
odps2-zljtm001	6
odps-zljtm002	2 8
mysql-parts	6
mysql-rds	6
ADS-zljtm001	6
odps-zljtm001	6

3. 在添加数据子集对话框的基本信息页签,输入子集名称、数据源、描述,单击下一步,如图 12-328: 添加数据子集基本信息所示。

图 12-328: 添加数据子集基本信息

		● 添加数据子集		×
基本信息 驱动表配置 数	居表配置			Î
	子集名称	子集名称		
	数 据 源	ADS1 •		1
	描述	描述		
				1
				•
			下一步取消	ă

4. 在添加数据子集对话框的驱动表配置页签,选择是否开启驱动配置表,单击下一步,如图 12-329: 添加数据子集驱动表配置所示。

图 12-329: 添加数据子集驱动表配置

				● 添加	加数据子集				×
基本	信息	驱动表配置	数据表配置						
★ 配置	驱动	动表可以自动添加相	关约束的数据	裱					
配置驱	动表	: 开启 关闭	模式:	模式		表名称:	表名称		搜索
选择	序号	模式		表名称	类	型	说	99	
0	1	datashield		datadiscoveryrule					
	2	sonar		project_qprofiles					
	3	sonar		properties					
	4	sonar		qprofile_changes					
۲	5	sonar		quality_gates					
K «	1	2 » N 🗌 🕻	<mark>60</mark> 每页 30	▼ 条 共32条					
							1	下₺	步 取消

开启配置驱动表后,可以选择所需要的驱动表。

5. 在添加数据子集对话框的数据表配置页签,勾选该子集所需要的表,单击保存,如图 12-330: 添加数据子集数据表配置所示。

图 12-330: 添加数据子集数据表配置

					◎ 添加数据				×
基本	信	息 驱动表配置	数据表配置						
模式:	1	模式	表	名称: 〔	表名称		□ 敏感表	搜索	
I A	多号	引模式	表名	称		类型		说明	
	1	datashield	data	discover	yrule				
	2	sonar	proje	ect_qpro	files				
	3	sonar	prop	erties					
	4	sonar	qpro	file_char	nges				
	5	sonar	quali	ty_gates	5				
	6	sonar	quali	ty_gate_	conditions				
₩ «	1	1 2 » N 🗌 Go	每页 30 🔻	条 共32身	Ř				
								上一步	保存 取消

12.5.3.3.1.2 编辑数据子集

操作步骤

1. 定位到**数据脱敏 > 数据子集**页面,选择已添加的数据子集,单击右侧的编辑按钮,如图 *12-331:* 数据子集列表所示。

图 12-331: 数据子集列表

数据子集列表	添加	删除
数据子集名称		T Q
□ 全选		
🔲 test		6
🔲 rds-tm		2
odps2-zljtm001		6
odps-zljtm002		2
mysql-parts		6
mysql-rds		6
ADS-zljtm001		2
odps-zljtm001		6

在编辑数据子集信息对话框中,修改该数据子集的基本信息、驱动表、及数据表配置等信息,如图 12-332:编辑数据子集信息所示。

图 12-332: 编辑数据子集信息

			✔ 编辑数据子集信息		×
基本信息	驱动表配置	数据表配置			Î
		子集名称	test		
		数 据 源	ADS1	•	
		描述	描述		
					Ŧ
				下一步取	Ť.
_					

说明: 数据子集的数据源无法修改。

12.5.3.3.1.3 删除数据子集

前提条件

删除数据子集前,请确认该数据子集与专有云数据安全系统中其它数据已无关联。

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 数据子集页面,选择已添加的数据子集,单击右侧的删除按钮,如图 12-333: 数据子集列表所示。

图 12-333: 数据子集列表

数据子集列表	添加	删除
数据子集名称		T Q
□ 全选		
🔲 test		2
🔲 rds-tm		2
odps2-zljtm001		6
odps-zljtm002		2
mysql-parts		6
mysql-rds		C 🗊
ADS-zljtm001		2
odps-zljtm001		6

3. 在信息提示对话框中,单击确定删除该数据子集。

12.5.3.3.2 数据关系

在执行数据发现任务时,如果启用了发现关系功能,发现任务执行完成后,具有主外键关联关系的 表将会在**数据关系**页面中展示相关约束及关系拓扑图。

12.5.3.3.2.1 查看数据关系

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 数据关系页面,单击数据表,查看该数据表的相关约束及关系拓扑图,如图 12-334:数据关系所示。

图 12-334: 数据关系

数据表列表		相关约束						
表名称	τq	序号 约束	名称	子表	父表	类型	输入类型	操作
* 🛢 ADS1 (1)		1 FK_AI	REA	ODC_PERSONINFO	ODC_AREA	外键	物理	٩
* 🛃 adstest (1)								
COC_AREA								
▼ 🛢 Odps数据库(3)								
) 🗟 dbsec (3)					^			
* 🛢 mysql-rds (3)		关系拓扑图	1					
) 🗮 test1 (3)		2000147144						
* 🗟 odps数据库2(1)								1
• 👼 dbsec2 (1)								
			SPENDINF	CARDINFO		ODC_AREA		
								-

12.5.3.3.3 脱敏方案

12.5.3.3.3.1 添加数据库脱敏方案

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据脱敏 > 脱敏方案页面,单击方案列表区域的添加,如图 12-335: 方案列表所示。

图 12-335: 方案列表

方案列表	添加		ЯЛ.	脉
方案名称			T	Q
□ ▼数据库方案	ł			
Odps	数据库			
□ i ≡ o	dps-zljtm001	۹	Ø	۵
	dps-zljtm002	۹	Ø	۵
□ * odps <u></u> ∦	收据库2			
	dsp2-zljtm001	Q	C	ŵ

- 3. 在添加方案对话框的基本信息页签中,输入方案名称、方案描述,选择数据类型为数据库,选择数据源,单击下一步,如图 12-336: 添加方案基本信息所示。
 - 图 12-336: 添加方案基本信息

				◎ 添加方	「家
基本信息	配置数据子集	配置默认算法	配置脱敞算法		
			方案名称	测试方窗1	
			数据源类型	数据库	٣
			数据源	ads-zljtm_test	٣
			脱敏方式	跨模式脱敏	•
			方案描述	方案描述	
i 🗐	兑明 :				
脱敏方象	案名称不可	「重复。			

4. 在添加方案对话框的配置数据子集页签中,选择数据子集,单击下一步,如图 12-337: 添加方案 配置数据子集所示。

送明:	
-----	--

输入数据子集名称,单击搜索,可查询相应的数据子集。

图 12-337: 添加方案配置数据子集

			O 添	珈方案		×
基	本信息	· 配置数据子集 配置默认算法	配置脱敏算法			
选择 数	数据于	华集到方案中: 集名称: 数据子集名称	搜索			
	序号	数据子集	数据源	驱动表	添加时间	1
	1	test	ADS1	zljtm001	2017-12-11 14:45:04	
	2	ADS-zljtm001	ADS1		2017-10-25 11:29:55	
						Ŧ
					上一步下一步取	硝

5. 在添加方案对话框的配置默认算法页签中,对敏感数据类型进行统一算法配置,单击下一

步,如图 12-338:添加方案配置默认算法所示。



您可以单击推荐算法,或手动选择脱敏算法并设置算法参数。
图 12-338: 添加方案配置默认算法

本信』	息 配置数据子集	配置默认算法 配置脱敏算法		
感数	屠类型进行统一算法配置	E:		
躬号	數据类型	脱敏算法	算法参数	当前算法
1	中文地址	中文地址替换	 ▼ 脱敏全部 ▼ 最大字节长度 255 	推荐算法
2	日期	日期替换	▼ 日期+时间 ▼ 年月日 ▼	推荐算法
3	Email地址	Email地址翻换	▼ 総敏全部 ▼	推荐算法
4	金额数字	金额数字随机	▼ 整数位数保留 ▼ 最小值 0 最大值 99	995 推荐算法
5	中文姓名	中文姓名曹操	▼ 脱敏全部 ▼	推荐算法
6	纳税人识别号	税号替换	Ŧ	推荐算法
7	企业名称组织机构	企业、组织机构名称曹操	*	推荐算法

- 在添加方案对话框的配置脱敏算法页签中,选择需要脱敏的数据表字段并配置脱敏算法,单击保存,如图 12-339:添加方案配置脱敏算法所示,完成添加脱敏方案。
 - 图 12-339: 添加方案配置脱敏算法

							◎ 添加7	方案				>
基	本信息	配置数据	子集	配置默认算法	配置脱线	改算法						ľ
筛	<u>ŧ</u> :			▼展开								
	模式	表名	字段	发现规则	样本	约束类型	脱敏算法		算法参数			当前算法
	adstest	zljtm001	addr	中文地址	内蒙古呼		中文地址曹换	٠	脱敏全部	٠	最大字节长度 255	推荐算法
	adstest	zljtm001	date	日期	2005/11/		日期曾换	•	日期+时间	٠	年月日	推荐算法
	adstest	zljtm001	email	Email地址	Aa23bb		Email地址替换	٣	脱敏全部	۲		推荐算法
	adstest	zljtm001	money	金额数字	122.23		金額数字随机	٣	整数位数保留	٠	最小值 0 最大值 99995	推荐算法
	adstest	zljtm001	name	中文姓名	李洪武		中文姓名曹换	٣	脱敏全部	۲		推荐算法
	adstest	zljtm001	nsrnum	纳税人识别	1101086		税号督换	٣				推荐算法
H	« 1 »	N	Go 每页	100 ▼ 条 共	11条							
											上一步	保存取消

12.5.3.3.3.2 添加文件脱敏方案

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据脱敏 > 脱敏方案页面,单击方案列表区域的添加,如图 12-340: 方案列表所示。

图 12-340: 方案列表

方第	羽表 添加		Đ	脉
2	方案名称		T	Q
	7 数据库方案			
	▼ Odps数据库			
	 ≡ odps-zljtm001	۹	Ø	Û
	 ≡ odps-zljtm002	۹	Ø	Û
	▼ odps数据库2			
	adsp2-zljtm001	۹	C	ŵ

- 3. 在添加方案对话框的基本信息页签中,输入方案名称、方案描述,选择数据类型为文件源,选择数据源,单击下一步,如图 12-341: 添加方案基本信息所示。
 - 图 12-341: 添加方案基本信息

				● 添加方案		×
基本信息	配置默认算法	配置脱敏算法				
			方案名称 数据源类型 数据 源	方案名称 文件源	•	
			方案描述	方案描述		
					下一步 取	肖



4. 在添加方案对话框的配置默认算法页签中,对敏感数据类型进行统一算法配置,单击下一

步,如图 12-342:添加方案配置默认算法所示。

说明:

您可以单击推荐算法,或手动选择脱敏算法并设置算法参数。

图 12-342: 添加方案配置默认算法

如感数的 家号	据类型进行统一算法配置 数据类型	能敏算法		算法参数					当前算法	
1	金额数字	金额数字随机	۲	整数位数保留	٠	最小值 0	最大值	99995	推荐算法	
2	手机号码	电话号码曹操	٣	脱敏后4位	٣				推荐算法	
3	中文姓名	中文姓名曹操	•	脱敏全部	٠				推荐算法	
4	中文地址	中文地址替换	٣	脱敏全部	٣	最大字节长度	255		推荐算法	
5	身份证号	身份证号替换	۲	脱敏地区	٠	脱敏生日	۲	脱敏性別・	推荐算法	
6	企业名称组织机构	企业、组织机构名称曹操	٣						推荐算法	
7	统一社会信用代码	统一社会信用代码随机	٣	脱敏机构类别	٠	脱敏地区		脱敏组织机构硕 🔻	推荐算法	

5. 在添加方案对话框的配置脱敏算法页签中,选择需要脱敏的文件数据列并配置脱敏算法,单击保存,如图 12-343: 添加方案配置脱敏算法所示,完成添加脱敏方案。

图 12-343: 添加方案配置脱敏算法

	● 添加方案 ×												
基本	本信息 配置默	人算法	配置脱	敗算法									
选	:		¥.	展开									
D	文件名	列序号	列标题	发现规则	样本	脱敏算法		算法参数					当前算法
1	zljtm001自定义	2		纳税人识别号	13010519	税号替换	۲						推荐算法
5	zljtm001自定义	4		手机号码	+8618623	电活号码替换	۲	脱椒后4位	۲				推荐算法
1	zljtm001自定义	5		座机号码	01023652	电活号码替换	۲	脱收后4位	۲				推荐算法
)	zljtm001自定义	6		中文姓名	张三丰	中文姓名替换	۳	脱敏全部	۲				推荐算法
)	zljtm001自定义	8		身份证号	10120219	身份证号替换	۳	脱敏地区	۲	脱敏生日・	脱敏性别	•	推荐算法
0	zljtm001自定义	9		企业名称组织机构	湖南京剧	企业、组织机构名	۲						推荐算法
(«1»)	Go æ	页 100	▼ 条 共10条									
												上一步	⇒ 保存 取

12.5.3.3.3.3 修改脱敏方案

背景信息

说明:

脱敏方案的方案名称、数据源类型、及数据源无法修改。

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据脱敏 > 脱敏方案页面。
- 3. 在**方案列表**区域中选择脱敏方案,单击右侧的编辑此方案信息按钮,如图 12-344: 方案列表所示。
 - 图 12-344: 方案列表



4. 在编辑方案对话框中,修改默认算法和脱敏算法,单击保存,如图 12-345:编辑脱敏方案所示。

图 12-345: 编辑脱敏方案

				✔ 编辑方案				
基本信息	配置数据子集	配置默认算法	配置脱敏算法					
			方案名称	odps-zljtm001				
			数据源类型	数据库	*			
			数 据 源	Odps数据库	*			
			脱敏方式	跨模式脱敏	٣			
			方案描述	方案描述				
							1	下一步

12.5.3.3.3.4 删除脱敏方案

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据脱敏 > 脱敏方案页面。
- 3. 在**方案列表**区域中选择脱敏方案,单击右侧的删除此方案信息按钮,如图 *12-346*:删除脱敏方案所示。

图 12-346: 删除脱敏方案

方	案列表 添加		₩	除
	方案名称		T	Q
	▼ 数据库方案			
	▼ Odps数据库			
	⊨ odps-zljtm001	۹	@	Û
	 ≡ odps-zljtm002	۹	C	ŵ
	▼ odps数据库2			
] ≡ odsp2-zljtm001	Q	C	ŵ

4. 在信息提示中,单击确定。

12.5.3.3.4 脱敏任务

专有云数据安全系统可以按照所选的脱敏算法,对已核实的数据库和文件源中的敏感数据进行脱 敏,并将脱敏结果存储到脱敏任务所指定的目的位置。

12.5.3.3.4.1 数据库脱敏任务

12.5.3.3.4.1.1 添加数据库脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据脱敏 > 脱敏任务页面,单击右上角的添加,如图 12-347: 脱敏任务列表所示。

图 12-347: 脱敏任务列表

脱敏任	务列表									55.20
运行	状态: 全部运行状态	•	脱敏任务名称:	脱敏任务名称	脱敏方案名称	家 : 脱敏方案名称	1	22 7 323		
序号	脱敏任务	任务进度	运行状态	5. 脱敏方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	-
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm001	数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:15:47	

3. 在添加脱敏任务对话框的基本信息页签,输入任务名称、任务描述,选择任务类型为数据库,选择码表,单击下一步,如图 12-348: 添加脱敏任务基本信息所示。

图 12-348: 添加脱敏任务基本信息

		● 添加脱敏任务		×
基本信息	选择脱敏方案 任务配置			
	任务名称	任务名称		
	任务类型	数据库	,	
	选择码表	CODE2016000000000	•	
	任务描述	描述		
			下一步 关	团

4. 在添加脱敏任务对话框的选择脱敏方案页签,勾选脱敏方案,在输出目的信息区域选择数据库类型,并选择目的数据库,填写数据库名及批量入库条数,单击下一步,如图 12-349:选择脱敏方案所示。



输出目的数据库的schema不能与数据库源的schema相同。

图 12-349: 选择脱敏方案

	● 添加脱敏任务	×
基本信息	选择脱敏方案 任务配置	
选择方案名称 方案名称:	方案名称 授家	
序号 选择	方案名称	
1 💮	ADS-zljtm001	
2 🔘	mysql-parts	
3 🔘	mysql-rds	
输出目的信息	p 98	
类 型:	● 数据库 ◎ 本地文件	
目的数据库	: mysql-rds2 * 数据库名: test2 批量入库: 100 条	
	上一步 下一步	关闭

5. 在添加脱敏任务对话框的任务配置页签,选择对象处理方式和异常处理方式,如图 *12-350*: 脱敏 任务配置所示,单击保存,完成该脱敏任务的添加。

图 12-350: 脱敏任务配置

● 添加脱敏任务	×
基本信息 选择脱敏方案 任务配置	
 対象处理: ● 创建对象之前先删除 ● 忽略对象已存在错误,插入前清空表数据 ● 忽略对象已存在错误,向表中追加数据 	
异常处理: 丢弃:异常数据所在的一整行将被丢弃(存在丢数据的风险) 置空:异常字段的值被置空,同行其他字段正常脱敏(该字段有非空约束时,该行数据将无法入库) 不变:异常字段的值保持不变,同行其他字段正常脱敏(存在敏感数据不变的风险) 	
注意:脱敏任务可能执行比较长的时间,请耐心等待。	
	// /171

12.5.3.3.4.1.2 执行数据库脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择已添加的数据库脱敏任务,单击任务记录右侧的操作列表,单击运行任务,如图 12-351: 脱敏任务列表所示。

图 12-351: 脱敏任务列表

脱敏任务 运行状	客列表 代态: 全部运行状态	* 脱敏行	[务名称: 脱敏 (1务名称	脱敏方案名称	脱敏方案名称	*	欧宗 下戦		添加
序号	脱敏任务	任务进度	运行状态	脱數方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	=
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm001	数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:1:	댼务
4	odps-zljtm002	100%	完成	odps-zljtm002	数据库	数据库	22222222	2017-11-06 11:06:17	2017-11-06 11:01 會 删除	上任务 余任务
5	mysql-parts	100%	完成	mysql-parts	数据库	数据库	22222222	2017-10-31 10:04:22	2017-10-31 10:04	服任务
6	mysql-rds	100%	完成	mysql-rds	数据库	数据库	22222222	2017-12-05 19:46:46	□ 万丈 2017-12-05 19:46.++7	2任务

- 3. 在运行脱敏任务对话框中,输入数据源的用户名、密码,输入输出源的用户名、密码,单击检测。
- 4. 检测通过后,单击运行,执行该脱敏任务,如图 12-352:运行脱敏任务所示。

图 12-352: 运行脱敏任务

	▶ 运行脱敏任务	×
数据源		
数据库	odps数据库1	
用户名	4NoJn9EvCm1oSPZR	
密码	•••••	
输出源		
数据库	odps数据库2	
用户名	4NoJn9EvCm1oSPZR	
密码	•••••	
	ž	西行 取消

等待该数据库脱敏任务执行完毕,如图 12-353: 脱敏任务运行完成所示。

图 12-353: 脱敏任务运行完成



12.5.3.3.4.1.3 停止数据库脱敏任务

背景信息

当数据库脱敏任务正在运行时,可以参考以下操作步骤,停止该脱敏任务:

操作步骤

1. 登录专有云数据安全控制台。

定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择正在运行的数据库脱敏任务,单击任务
 记录右侧的操作列表,单击停止任务,如图 12-354:停止脱敏任务所示。

图 12-354: 停止脱敏任务

脱敏任务列表										添加
运行	大态: 全部运行状态	▼ 脱敏任	务名称:脱敏(E务名称	脱敏方案名称:	脱敏方案名称	19 <i>%</i> :	下载		
序号	脱敏任务	任务进度	运行状态	脱敏方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	=
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm001	数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:15	▶ 运行任务
4	odps-zljtm002	100%	完成	odps-zljtm002	数据库	数据库	22222222	2017-11-06 11:06:17	2017-11-06 11:0;	會删除任务
5	mysql-parts	100%	完成	mysql-parts	数据库	数据库	22222222	2017-10-31 10:04:22	2017-10-31 10:04	2 编辑任务
6	mysql-rds	100%	完成	mysql-rds	数据库	数据库	22222222	2017-12-05 19:46:46	2017-12-05 19:46.++	

3. 在信息提示对话框中,单击确定。

12.5.3.3.4.1.4 查看数据库脱敏任务的历史任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择已完成的数据库脱敏任务,单击任务记录右侧的操作列表,单击历史任务,如图 12-355: 脱敏任务列表所示。

图 12-355: 脱敏任务列表

脱敏任务列表										添加
运行机	大态 : 全部运行状态	▼ 脱敏台	务名称: 脱敏信	[务名称	脱敏方案名称:	脱敏方案名称	按索	下蛇		
序号	脱敏任务	任务进度	运行状态	脱敏方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	=
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm001	数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:15	▶ 运行任务
4	odps-zljtm002	100%	完成	odps-zljtm002	数据库	数据库	22222222	2017-11-06 11:06:17	2017-11-06 11:03	自删除任务
5	mysql-parts	100%	完成	mysql-parts	数据库	数据库	22222222	2017-10-31 10:04:22	2017-10-31 10:04	☞ 編編任务
6	mysql-rds	100%	完成	mysql-rds	数据库	数据库	22222222	2017-12-05 19:46:46	2017-12-05 19:46.47	國历史任务

3. 在**脱敏任务执行记录**对话框中,选择已执行的任务记录,单击执行报告按钮,如图 *12-356*: 脱敏 任务执行记录所示。

图 12-356: 脱敏任务执行记录

	☰ 脱敏任务执行记录										
0 4 36-	22 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2										
任务号	任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作					
346	100%	完成	22222222	2017-09-07 17:35:11	2017-09-07 17:35:33	b ± 0					
345	100%	完成	22222222	2017-09-07 17:34:13	2017-09-07 17:34:30	8 ≜ ⊙					
344	100%	完成	22222222	2017-09-07 17:18:08	2017-09-07 17:18:31	∎ ≛ ⊚					
342	100%	完成	22222222	2017-09-07 17:05:41	2017-09-07 17:06:04	8 ≛ ⊙					
341	100%	完成	22222222	2017-09-07 17:01:55	2017-09-07 17:02:47	■ ▲ ⊙					
340	100%	完成	22222222	2017-09-07 16:51:45	2017-09-07 16:52:08	8 ≛ ⊙					
331	100%	完成	22222222	2017-09-07 14:55:29	2017-09-07 14:55:44	∎ ▲ ⊙					
н 🔐 1	» N Go 每页 30 ▼ 条 共9条	-to-state	******			• • •					
						*10					

4. 在脱敏任务执行报告页面,查看该脱敏任务的执行报告,如图 12-357: 脱敏任务执行报告所示。

图 12-357: 脱敏任务执行报告

脱敏任务执行报告							
基本信息							
任务名称: odps-zljtm001			任务运行时间	司: 22秒326電秒			
任务总对象数(表/文件):1			脱敏对象数	(悫/文件): 1			
任务总记录数: 10			脱敏记录数	: 0			
任务总列数(字段/文件列): 13			脱敏列数 (考	纬段/文件列): 13	3		
脱敏任务执行信息							
执行信息列表							执行
运行状态: 全部运行状态 ·	模式名: 模式名	表名:	表名	搜索	I		
□ 序号 数据源 模式	表 运行状态	总列数 脱氧	如何数 总行	行数 脱敏行数	脱敏异常行	入库行数	入库异常行数
1 odps数据率1 dbsec	zljtm001 完成	13	13 1	0 0	10	10	0
K « 1 » X Go 每页 :	30 • 条 共1条						
异常日志列表							
日志级别: 全部 •	错误名 : 错误名	表名:	表名	搜索	l i		
序号 错误名称	严重级别 表名	任务号	任务类别(普误详细信息		B	晌
1 字段脱敏失败	警告 zljtm001	346	脱軟任务	見数异常:column:日期	index:12,v	2017-09	07 17:35:30
2 字段脱散失败	警告 zljtm001	346	脱敏任务	电影子和:column:日期	index:12,v	2017-09	07 17:35:30
3 李段脱散失败	警告 zljtm001	346	脱敏任务 1	总数异常:column:日期	(index:12,v	2017-09	07 17:35:30
4 字段脱敏失败	警告 zljtm001	346	脱敏任务	说数异常:column:日期	lindex:12,v	2017-09	07 17:35:30
K 《 1 》 X 🗌 😡 每页 🗄	30 🔹 条 共10条						

12.5.3.3.4.1.5 编辑数据库脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择数据库脱敏任务,单击任务记录右侧的 操作列表,单击编辑任务,如图 12-358: 脱敏任务列表所示。

图 12-358: 脱敏任务列表

脱散任务列表										添加
运行机	太 态: 全部运行状态	▼ 脱敏台	务名称: 脱敏信	[务名称	脱敏方案名称:	脱敏方案名称	搜索	下载		
序号	脱敏任务	任务进度	运行状态	脱敏方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	=
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm001	数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:15	▶ 运行任务
4	odps-zljtm002	100%	完成	odps-zljtm002	数据库	数据库	22222222	2017-11-06 11:06:17	2017-11-06 11:0	● ● 単独任务
5	mysql-parts	100%	完成	mysql-parts	数据库	数据库	22222222	2017-10-31 10:04:22	2017-10-31 10:04	☞ 編編任务
6	mysql-rds	100%	完成	mysql-rds	数据库	数据库	22222222	2017-12-05 19:46:46	2017-12-05 19:46:+7	

3. 在编辑脱敏任务对话框中,变更码表、任务描述、输出目的数据库信息、对象处理方式、异常处理方式,单击保存,如图 12-359:编辑脱敏任务所示。



任务名称、任务类型无法修改。

图 12-359: 编辑脱敏任务

		✔ 编辑脱敏任务		×
基本信息 选择脱	嫩方案 任务配置			
	任务名称	rds-mysql		
	任务类型	数据库	v	
	选择码表	CODE20171026144103	•	
	任务描述	描述		
			<u><u> </u></u>	的
			2 V - 2	CIAI

12.5.3.3.4.1.6 删除数据库脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择数据库脱敏任务,单击任务记录右侧的 操作列表,单击删除任务,如图 12-360: 删除脱敏任务所示。

图 12-360: 删除脱敏任务

N數在务列表										添加
运行物	t态: 全部运行状态	▼ 脱敏白	务名称:脱敏信	[务名称	脱敏方案名称:	脱敏方案名称	12:8	: 下载		
序号	脱敏任务	任务进度	运行状态	脱敏方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	=
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm001	数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:1:	▶ 运行任务
4	odps-zljtm002	100%	完成	odps-zljtm002	数据库	数据库	22222222	2017-11-06 11:06:17	2017-11-06 11:0:	自删除任务
5	mysql-parts	100%	完成	mysql-parts	数据库	数据库	22222222	2017-10-31 10:04:22	2017-10-31 10:04	☞ 编辑任务
6	mysql-rds	100%	完成	mysql-rds	数据库	数据库	22222222	2017-12-05 19:46:46	2017-12-05 19:46.44	面 历史任务

3. 在信息提示对话框中,单击确定,删除该脱敏任务。

12.5.3.3.4.2 文件脱敏任务

12.5.3.3.4.2.1 添加文件脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到数据脱敏 > 脱敏任务页面,单击右上角的添加,如图 12-361: 脱敏任务列表所示。

图 12-361: 脱敏任务列表

脱敏任务列表										
运行状	志: 全部运行状态	•	脱散任务名称:	脱敏任务名称	脱敏方案名称	: 脱敏方案名称	1	28 F5		
序号	脱敏任务	任务进度	运行状	态 脱敏方案	源类型	输出类型	添加用户	添加时间	上次完成时间	操作
1	zljtm002.txt	100%	完成	zljtm002.txt	文件	数据库	22222222	2017-11-08 14:24:11	2017-11-08 14:24:11	
2	rds-mysql	100%	完成	rds-tm	数据库	数据库	22222222	2017-11-08 14:19:38	2017-11-08 14:19:39	-
3	ODPS2-zljtm001	100%	完成	odsp2-zljtm00	1 数据库	文件	22222222	2017-11-08 14:15:00	2017-11-08 14:15:47	-

3. 在**添加脱敏任务**对话框的基本信息页签,输入任务名称、任务描述,选择任务类型为文件,选择码表,单击**下一步**,如图 *12-362*: 添加脱敏任务基本信息所示。

图 12-362: 添加脱敏任务基本信息

	● 添加脱敏任务	×
基本信息 选择脱敏方案 任务配置		
任冬冬森	样冬夕珠	
任务举型	文件 •	
选择码表	CODE201600000000 T	
任务描述	描述	
		下一步 关闭

4. 在添加脱敏任务对话框的选择脱敏方案页签,勾选脱敏方案,在输出目的信息区域选择本地文件
 类型,单击下一步,如图 12-363:选择脱敏方案所示。

图 12-363: 选择脱敏方案

					● 添加脱敏任务	×
基本	信息	选择制	脫放方案	任务配置		
选择所 方	京案名称 案名称	K : 万案	名称		授索	
	序号	选择	方案名	称		
	1	۲	zljtm00	1.txt		1
60	2	0	zljtm00	1自定义.txt		
-	3	\odot	zljtm00	1自定义1.txt		1
输出E 类	型	1. : ◎ 数	刘据库 💽	本地文件		
					上一步 下一	步

5. 在**添加脱敏任务**对话框的**任务配置**页签,选择异常处理方式,如图 *12-364*: 添加脱敏任务任务配置所示,单击**保存**,完成该脱敏任务的添加。

图 12-364: 添加脱敏任务任务配置

● 添加脱敏任务	×
基本信息 选择脱散方案 任务配置	
异常处理: ② 丢弃:异常数据所在的一整行将被丢弃(存在丢数据的风险) ③ 置空:异常字段的值被置空,同行其他字段正常脱敏(该字段有非空约束时,该行数据将无法入库) ③ 不变:异常字段的值保持不变,同行其他字段正常脱敏(存在敏感数据不变的风险)	
注意:脱敏任务可能执行比较长的时间,请耐心等待。	
上一步保存保存并运行	关闭

12.5.3.3.4.2.2 执行文件脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择已添加的文件脱敏任务,单击任务记录 右侧的操作列表,单击运行任务,如图 12-365: 脱敏任务列表所示。

图 12-365: 脱敏任务列表

7	zljtm001自定义1.txt	100%	完成	zljtm001自定义1.txt	文件	文件	22222222	2017-12-11 18:19:09 2017-12-11 18:19:10
8	zljtm001自定义.txt	100%	完成	zljtm001自定义.txt	文件	数据库	22222222	2017-10-27 13:57:34 2017-10-27 13:5
9	zljtm001.txt	100%	完成	zljtm001.txt	文件	文件	22222222	2017-10-30 11:00:33 2017-10-30 11:00 會勝除任务
10	ADS-zljtm001	100%	完成	ADS-zljtm001	数据库	文件	22222222	2017-10-25 13:52:21 2017-10-25 13:52 译 编辑任务
11	odps-zljtm001	100%	完成	odps-zljtm001	数据库	数据库	22222222	2017-10-26 10:06:38 2017-10-26 10:08.00

- 3. 在运行脱敏任务对话框中,单击检测。
- 4. 检测通过后,单击运行,如图 12-366: 运行脱敏任务所示,执行该脱敏任务。

图 12-366: 运行脱敏任务

▶ 运行脱敏任	务 ×
检测列表 1.文件是否存在	⊘成功
2.目标磁盘空间检测	⊘ 成功
	运行取消

12.5.3.3.4.2.3 停止文件脱敏任务

背景信息

当文件脱敏任务正在运行时,可以参考以下操作步骤,停止该脱敏任务:

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择正在运行的文件脱敏任务,单击任务记录右侧的操作列表,单击停止任务,如图 12-367:停止脱敏任务所示。

图 12-367: 停止脱敏任务

7	zljtm001自定义1.txt	100%	完成	zljtm001自定义1.txt	文件	文件	22222222	2017-12-11 18:19:09 2017-12-11 18:19:10
8	zljtm001自定义.txt	100%	完成	zljtm001自定义.txt	文件	数据库	22222222	2017-10-27 13:57:34 2017-10-27 13:5
9	zljtm001.txt	100%	完成	zljtm001.txt	文件	文件	22222222	2017-10-30 11:00:33 2017-10-30 11:0(會劇除任务
10	ADS-zljtm001	100%	完成	ADS-zljtm001	数据库	文件	22222222	2017-10-25 13:52:21 2017-10-25 13:5; 译编辑任务
11	odps-zljtm001	100%	完成	odps-zljtm001	数据库	数据库	22222222	2017-10-26 10:06:38 2017-10-26 10:08:00

3. 在信息提示对话框中,单击确定。

12.5.3.3.4.2.4 查看文件脱敏任务的历史任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择已完成的文件脱敏任务,单击任务记录 右侧的操作列表,单击历史任务,如图 12-368: 脱敏任务列表所示。

图 12-368: 脱敏任务列表

7	alitem001白史以1.txt	100%	金成	zlitm001白史以1 tvt	77.87	***	2222222	2017-12-11 19:19:09 2017-12-11 19:19:10
'	2junoor Bizzk nav	10070	70.00	ZIJUNOTE ZA NAV	XH.	217	LLLLLLL	2017-12-11 10.13.03 2017-12-11 10.13.10
8	zljtm001自定义.txt	100%	完成	zljtm001自定义.txt	文件	敗掘库	22222222	2017-10-27 13:57:34 2017-10-27 13:5:
9	zljtm001.txt	100%	完成	zljtm001.txt	文件	文件	22222222	2017-10-30 11:00:33 2017-10-30 11:00 C MIN/LS
10	ADS-zljtm001	100%	完成	ADS-zljtm001	数据库	文件	22222222	2017-10-25 13:52:21 2017-10-25 13:52
11	odps-zljtm001	100%	完成	odps-zljtm001	数据库	数据库	22222222	2017-10-26 10:06:38 2017-10-26 10:08:00

3. 在**脱敏任务执行记录**对话框中,选择已执行的任务记录,单击执行报告按钮,如图 *12-369*: 脱敏 任务执行记录所示。

图 12-369: 脱敏任务执行记录

			≡ 脱敏任务执行记录			×
0 🕬						按索
任务号	任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作
334	100%	完成	22222222	2017-09-07 15:54:08	2017-09-07 15:54:09	■ ▲ ⊚
333	100%	完成	22222222	2017-09-07 15:49:56	2017-09-07 15:49:57	∎ ≛ ⊚
332	100%	完成	22222222	2017-09-07 15:32:05	2017-09-07 15:34:08	∎ ≛ ⊚
H «	1 » N 🚺 👍 每页 30 🔹 条 共3条					
						564

4. 在脱敏任务执行报告页面,查看该脱敏任务的执行报告,如图 12-370: 脱敏任务执行报告所示。

图 12-370: 脱敏任务执行报告

脱敏任务执行报告							
基本信息							
任务名称: ads-zljtm_test			任务运行时间	同: 1秒416電秒			
任务总对象数(表/文件):1		ļ	脱散对象数((表/文件):1			
任务总记录数: 10)	脱敏记录数:	: 10			
任务总列数(字段/文件列):13		ļ	脱敝列数(书	解 () : 13	1		
脱敏任务执行信息							
执行信息列表							th C
941716257938							201
运行状态: 全部运行状态 🔻	模式名: 模式名	表名:	表名	2020k			
□ 序号 数据源 模式	表 运行状态	总列数 脱敏	別数 总行	示数 脱敏行数	脱敏异常行	入库行数	入库异常行数
1 ads-zljtm_t adstest	tm_test 完成	13 13	3 10	0 10	0	0	0
K «1 ») Go 每页 3	0 ▼)条 共1条						
异常日志列表							
日志级别: 全部 v	错误名: 错误名	表名:	表名	21:11:			
序号 错误名称	严重级别 表名	任务号	任务类别 错	盐误详细信息		B	銄
		无数据					

5. 在**脱敏任务执行记录**对话框中,选择已执行的任务记录,单击FTP下载按钮,如图 *12-371:* 下载 脱敏后的文件所示,可下载脱敏后的文件。

图 12-371: 下载脱敏后的文件

	■ 脱氧任务执行记录										
 ● 載近一用 											
任務号 6	任务进度	运行状态	执行用户	执行开始时间	执行结束时间	操作					
334 1	100%	完成	22222222	2017-09-07 15:54:08	2017-09-07 15:54:09	∎ <u>▲</u> ⊚					
333 1	100%	完成	22222222	2017-09-07 15:49:56	2017-09-07 15:49:57	∎ ≛ ⊜					
332 1	100%	完成	22222222	2017-09-07 15:32:05	2017-09-07 15:34:08	▲ ④					
H « 1 :	» N 🚺 🐻 每页 30 🔻 景 共3条										
						_					

12.5.3.3.4.2.5 编辑文件脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择文件脱敏任务,单击任务记录右侧的操作列表,单击编辑任务,如图 12-372: 脱敏任务列表所示。

图 12-372: 脱敏任务列表

7	zljtm001自定义1.txt	100%	完成	zljtm001自定义1.txt	文件	文件	22222222	2017-12-11 18:19:09 2017-12-11 18:19:10
8	zljtm001自定义.txt	100%	完成	zljtm001自定义.txt	文件	数据库	22222222	2017-10-27 13:57:34 2017-10-27 13:5: 医行任务
9	zljtm001.txt	100%	完成	zljtm001.txt	文件	文件	22222222	2017-10-30 11:00:33 2017-10-30 11:00 含節除任务
10	ADS-zljtm001	100%	完成	ADS-zljtm001	数据库	文件	22222222	2017-10-25 13:52:21 2017-10-25 13:5; 2 编辑任务
11	odps-zljtm001	100%	完成	odps-zljtm001	数据库	数据库	22222222	2017-10-26 10:06:38 2017-10-26 10:08:00

3. 在编辑脱敏任务对话框中,变更码表、任务描述、输出目的、对象处理方式、异常处理方式,单击保存,如图 12-373:编辑脱敏任务所示。



图 12-373: 编辑脱敏任务

✔ 编辑脱敏任务	×
基本信息 选择脱敏方案 任务配置	
 対象处理: ● 插入前清空表数据 ● 向表中追加数据 	
异常处理: 丢弃:异常数据所在的一整行将被丢弃(存在丢数据的风险) ● 置空:异常字段的值被置空,同行其他字段正常脱敏(该字段有非空约束时,该行数据将无法入库) ● 不变:异常字段的值保持不变,同行其他字段正常脱敏(存在敏感数据不变的风险) 	
注意:脱敏任务可能执行比较长的时间,请耐心等待。	
上一步保存 保存并运行	关闭

12.5.3.3.4.2.6 删除文件脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,在脱敏任务列表中选择文件脱敏任务,单击任务记录右侧的操作列表,单击删除任务,如图 12-374: 删除脱敏任务所示。

图 12-374: 删除脱敏任务

7	zljtm001自定义1.txt	100%	完成	zljtm001自定义1.txt	文件	文件	22222222	2017-12-11 18:19:09 2017-12-11 18:19:10
8	zljtm001自定义.txt	100%	完成	zljtm001自定义.txt	文件	数据库	22222222	2017-10-27 13:57:34 2017-10-27 13:5: 医疗任务
9	zljtm001.txt	100%	完成	zljtm001.txt	文件	文件	22222222	2017-10-30 11:00:33 2017-10-30 11:0(會勝降任务
10	ADS-zljtm001	100%	完成	ADS-zljtm001	数据库	文件	22222222	2017-10-25 13:52:21 2017-10-25 13:5; 2 编辑任务
11	odps-zljtm001	100%	完成	odps-zljtm001	数据库	数据库	22222222	2017-10-26 10:06:38 2017-10-26 10:08.vo

3. 在信息提示对话框中,单击确定,删除该脱敏任务。

12.5.3.3.4.3 查询脱敏任务

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏任务页面,选择运行状态、输入脱敏任务名称,单击搜索,如图 12-375: 搜索脱敏任务所示,查询符合相应条件的所有脱敏任务。

图 12-375: 搜索脱敏任务

脱敏任务列表							
运行状态:	全部运行状态	脱敏任务名称:	脱敏任务名称	脱敏方案名称:	脱敏方案名称	搜索	下载

12.5.3.3.5 脱敏算法

专有云数据安全内置了53种脱敏算法,用于对已核实的数据库和文件源中的敏感数据进行脱敏。

12.5.3.3.5.1 查看脱敏算法

操作步骤

- 1. 登录专有云数据安全控制台。
- 定位到数据脱敏 > 脱敏算法页面,在脱敏算法列表区域选择脱敏算法记录,右侧的脱敏算法信息
 区域将展示该脱敏算法的详细信息,如图 12-376: 查看脱敏算法所示。

图 12-376: 查看脱敏算法

脱敏算法列表	添加	脱敏算法信息			脱敏算法测试		
脱敏算法名称	٩	算法名称: 证件号替换(含身	份证、军官证、		码表文件选择:	CODE2016000000000	,
7 内置算法		算法类型:基础脱散算法	v 🚯		输入样本数据:	测试数据样本	
身份证号替换		是否可逆: • 可逆 • 不可论	● 可逆 ○ 不可逆		输出脱敏数据:	数据脱敏结果	
身份证号随机		算法描述:除包含身份证号码 外,对于其他证件	」 替换脱散算法规则 「 号采用数字替换方			脱敏测试	
证件号替换(含身份		式并保留特征字符					
证件号随机(含身份		脱敏参数					
银行卡号信用卡号蓄换		・ 脱敏参数选择 脱敏地区 ・ 脱敏生日 ・ 脱敏性別 ・ つ 日					
银行卡号信用卡号随机							

3. 在脱敏算法测试区域,选择码表文件,输入测试数据,单击**脱敏测试**,在输出脱敏数据框中可显示测试样本脱敏后的数据。

12.5.3.3.5.2 添加自定义脱敏算法

操作步骤

- 1. 登录专有云数据安全控制台。
- 2. 定位到**数据脱敏 > 脱敏算法**页面,在脱敏算法列表区域单击**添加**,如图 *12-377:* 添加脱敏算法所示。
 - 图 12-377: 添加脱敏算法

脱散算法列表 1810 脱散算法名称 Q	脱軟算法信息 脱軟算法测试 算法名称: 脱款算法名称:	保存
 内置算法 身份证号構施 身份证号循机 	算法类型: 复合脱放算法 ● 最否可逆: ● 第 ● 第 ● 第 ● ● ● <th></th>	
运件每据换(含身份 运件号据机(含身份 银行卡号信用卡号器换 银行卡号信用卡号器换	脱散参数 复合发现规则: 复合-按位 • 斯分方式: 按位新分	
电话号码器块 电话号码器块 手机号码器块	序号 名称 开始位 结束位 分段样本 基础算法 算法参数 ● F.REGR	

3. 在脱敏算法信息、脱敏参数、脱敏算法测试区域设置自定义算法的相关信息,单击保存。