ALIBABA CLOUD

阿里云

专有云企业版

云盾

用户指南

产品版本：V3.16.1

文档版本：20220429

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。

1. 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。

2. 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。

3. 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. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，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、发行或公开发表阿里云网站、产品程序或内容。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. 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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *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。	`switch {active|stand}`

目录

1.什么是云盾 32
2.使用须知 34
3.快速入门 35
3.1. 用户权限说明 35
3.2. 登录云盾安全中心 35
4.态势感知 37
4.1. 概述 37
4.2. 总览 37
4.2.1. 查看安全总览信息 37
4.2.2. 查看安全大屏 38
4.3. 安全告警 41
4.3.1. 查看安全告警 41
4.3.2. 管理文件隔离箱 42
4.3.3. 安全告警设置 43
4.4. 攻击分析 46
4.5. 云产品检查 47
4.5.1. 云产品检查概述 47
4.5.2. 执行云产品检查 50
4.5.3. 查看和处理云产品检查结果 51
4.6. 资产中心 53
4.6.1. 查看服务器安全状态 53
4.6.2. 查看云产品安全状态 55
4.6.3. 查看单个资产详情 57
4.6.4. 开启和关闭服务器保护状态 61
4.6.5. 一键安全检查 61
4.6.6. 管理资产分组 62

4.6.7. 管理资产标签 65
4.7. 应用白名单 68
4.8. 漏洞扫描 70
4.8.1. 快速入门 70
4.8.2. 查看概览 71
4.8.3. 资产管理 72
4.8.3.1. 查看资产分析 72
4.8.3.2. 导入资产 74
4.8.3.3. 管理资产列表 75
4.8.3.4. 管理资产可用性 78
4.8.3.5. 管理自定义更新检测 80
4.8.4. 风险管理 82
4.8.4.1. 管理安全漏洞风险 82
4.8.4.2. 管理主机合规风险 83
4.8.4.3. 管理外部风险 84
4.8.4.4. 创建自定义风险检测 85
4.8.5. 报表管理 85
4.8.5.1. 创建报表 85
4.8.5.2. 批量删除报表 87
4.8.6. 配置管理 87
4.8.6.1. 配置全局监控 87
4.8.6.2. 配置基础监控 90
4.8.6.3. 配置Web监控 95
4.8.6.4. 配置白名单 97
4.8.6.5. 配置扫描引擎（私有资产） 98
4.9. 安全报告 99
5.网络流量检测与响应 101
5.1. 查看流量趋势 101

5.2. 查看互联网边界流量 101
5.3. 查看内网边界流量 103
5.4. 管理网络抓包任务 104
5.5. 日志检索 105
5.6. 攻击者画像 106
5.7. 威胁检测 108
5.7.1. 威胁检测 108
5.7.2. 查看封禁日志 110
5.8. 行为分析 112
5.8.1. 加密流量分析 112
5.8.2. DNS行为分析 113
5.9. 配置策略 114
5.9.1. 配置网络层策略 114
5.9.2. 配置应用层策略 116
5.9.3. 配置端口扫描欺骗策略 119
5.9.4. 管理地址簿 121
6.主机安全 124
6.1. 主机安全总览 124
6.2. 主机指纹 124
6.2.1. 管理监听端口 124
6.2.2. 管理软件版本 125
6.2.3. 管理运行进程 125
6.2.4. 管理账号信息 126
6.2.5. 管理计划任务 126
6.2.6. 设置主机指纹采集频率 126
6.3. 安全预防 127
6.3.1. 漏洞管理 127
6.3.1.1. 管理Linux软件漏洞 127

6.3.1.2. 管理Windows系统漏洞 128
6.3.1.3. 管理Web-CMS漏洞 128
6.3.1.4. 管理应急漏洞 129
6.3.1.5. 设置漏洞管理策略 130
6.3.2. 基线检查 131
6.3.2.1. 基线检查介绍 131
6.3.2.2. 设置基线检查策略 134
6.3.2.3. 查看和处理基线检查结果 135
6.4. 入侵防护 138
6.4.1. 入侵事件 138
6.4.1.1. 入侵事件类型概述 138
6.4.1.2. 查看和处理入侵事件 139
6.4.1.3. 查看告警自动化关联分析 140
6.4.1.4. 文件隔离箱 141
6.4.1.5. 安全告警设置 141
6.4.1.6. 病毒云查杀 142
6.4.2. 网页防篡改 144
6.4.2.1. 概述 144
6.4.2.2. 创建网页防篡改保护 145
6.4.2.3. 查看防护状态 148
6.4.3. 病毒查杀 149
6.5. 日志检索 150
6.5.1. 日志检索介绍 150
6.5.2. 查询日志 151
6.5.3. 各日志源字段说明 152
6.5.4. 语法逻辑说明 155
6.6. 设置 156
6.6.1. 安装客户端 156

6.6.2. 管理防护模式 157
7.物理机主机安全 159
7.1. 创建和授权账号 159
7.2. 主机列表 160
7.2.1. 管理分组 160
7.2.2. 管理主机列表 162
7.3. 入侵事件 162
7.3.1. 入侵事件类型概述 162
7.3.2. 查看和处理入侵事件 164
7.3.3. 查看告警自动化关联分析 165
7.3.4. 文件隔离箱 165
7.3.5. 安全告警设置 166
7.3.6. 病毒云查杀 167
7.4. 主机指纹 168
7.4.1. 管理监听端口 168
7.4.2. 管理软件版本 169
7.4.3. 管理运行进程 169
7.4.4. 管理账号信息 169
7.4.5. 管理计划任务 170
7.4.6. 设置主机指纹采集频率 170
7.5. 日志检索 170
7.5.1. 各日志源字段说明 170
7.5.2. 语法逻辑说明 174
7.5.3. 查询日志 175
7.6. 配置物理机安全 176
8.应用安全 177
8.1. 快速入门 177
8.2. 防护总览 177

8.2.1. 查看防护总览 177
8.2.2. 查看访问状态监控 178
8.3. 防护日志 179
8.3.1. 查看攻击检测日志 179
8.3.2. 查看CC防护日志 179
8.3.3. 查看BOT验证日志 180
8.3.4. 查看系统操作日志 180
8.3.5. 查看访问日志 180
8.4. 防护配置 181
8.4.1. 配置防护策略 181
8.4.2. 配置自定义规则 182
8.4.3. 配置CC防护规则 184
8.4.4. 配置CC白名单 187
8.4.5. 配置BOT防护 188
8.4.6. 上传证书 191
8.4.7. 添加互联网防护站点 191
8.4.8. 添加VPC防护站点 197
8.4.9. 本地验证域名接入配置 201
8.4.10. 修改DNS解析 201
8.5. 系统管理 202
8.5.1. 查看节点负载状态 202
8.5.2. 查看节点网络状态 203
8.5.3. 查看节点磁盘状态 204
8.5.4. 配置告警服务 205
8.5.5. 配置告警阈值 206
9.云安全管理中心（SOC） 208
9.1. 运营中心 208
9.2. 态势监控 211

9.3. 风险分析 213
9.3.1. 查看威胁事件 213
9.3.2. 查看弱点分析数据 213
9.3.3. 查看流量分析数据 215
9.3.4. 查看威胁情报 215
9.4. 资产管理 216
9.4.1. 查看租户资产 217
9.4.2. 查看平台资产 217
9.5. 日志管理 219
9.5.1. 查看日志概览 219
9.5.2. 查询原始日志 221
9.5.3. 查看平台日志 222
9.5.4. 查看租户日志 223
9.5.5. 日志配置 225
9.5.5.1. 管理日志源 225
9.5.5.2. 设置日志解析模板 226
9.5.5.3. 设置日志转发 227
9.6. 管理报表 228
9.7. 规则管理 229
9.7.1. 分析规则 229
9.7.2. 封禁规则 231
9.8. 运营管理 232
9.8.1. 安全审计 232
9.8.1.1. 概述 232
9.8.1.2. 查看审计汇总信息 232
9.8.1.3. 查询审计事件 234
9.8.1.4. 查看原始日志 235
9.8.1.5. 查看日志量 235

9.8.1.6. 策略设置 236
9.8.1.6.1. 管理审计规则 236
9.8.1.6.2. 设置告警接收人 238
9.8.1.6.3. 查询事件日志存档 238
9.8.1.6.4. 下载导出的任务 239
9.8.1.6.5. 修改系统配置 240
9.8.2. 配置存储策略 240
9.8.3. 新增自定义IP地址和地理位置 241
10.可选安全产品 242
10.1. DDoS防护 242
10.1.1. 概述 242
10.1.2. 查看和配置DDoS防护策略 242
10.1.3. 查看DDoS流量清洗事件 244
10.2. 云防火墙 245
10.2.1. 策略配置 245
10.2.1.1. 互联网边界防火墙同步资产 245
10.2.1.2. 创建VPC边界防火墙 245
10.2.1.3. 创建IDC-VPC边界防火墙 247
10.2.2. 访问控制 250
10.2.2.1. 管理地址簿 250
10.2.2.2. 配置互联网边界防火墙 252
10.2.2.3. 新增策略组 255
10.2.2.4. 配置主机边界防火墙访问控制策略 255
10.2.2.5. 配置VPC边界防火墙访问控制策略 258
10.2.2.6. 配置IDC-VPC边界防火墙访问控制策略 261
10.2.3. 入侵防御 263
10.2.3.1. 配置入侵防御策略 263
10.2.3.2. 查看IPS拦截记录 265

10.2.4. 查看安全组 269
10.2.5. 日志审计 273
10.2.5.1. 查看事件日志 273
10.2.5.2. 查看流量日志 274
10.3. 数据库审计 275
10.3.1. 概述 275
10.3.2. 快速部署指南 276
10.3.2.1. 部署数据库审计系统 276
10.3.2.2. 配置自定义IP 277
10.3.2.3. 登录数据库审计系统（云盾安全中心登录） 278
10.3.2.4. 数据库审计系统初始化 278
10.3.2.4.1. 前提条件 278
10.3.2.4.2. 导入License文件 279
10.3.2.4.3. 添加被审计的数据库实例 279
10.3.2.4.4. 部署Agent程序 280
10.3.2.4.4.1. 自动部署 280
10.3.2.4.4.2. Windows系统手动部署（应用服务与数据库服务器.. 281
10.3.2.4.4.3. Windows系统手动部署（应用服务与数据库服务器.. 283
10.3.2.4.4.4. Windows系统服务器修改Agent程序连接地址 285
10.3.2.4.4.5. Linux系统手动部署（应用服务与数据库服务器不... 286
10.3.2.4.4.6. Linux系统手动部署（应用服务与数据库服务器相... 287
10.3.2.4.4.7. Linux系统服务器修改Agent程序连接地址 289
10.3.2.4.5. 部署测试 290
10.3.3. 系统管理员指南 290
10.3.3.1. 概述 290
10.3.3.2. 系统管理 291
10.3.3.2.1. 通知管理 291
10.3.3.3. 监控管理 291

10.3.3.3.1. 压力 291
10.3.3.3.2. 资源与引擎 292
10.3.3.3.3. 数据中心监控 293
10.3.3.3.4. 网络流量监控 293
10.3.3.3.5. 异常日志 294
10.3.3.3.6. 系统日志 294
10.3.3.3.7. 调度日志 295
10.3.4. 安全管理员指南 295
10.3.4.1. 概述 295
10.3.4.2. 概况 296
10.3.4.2.1. 系统检测 296
10.3.4.2.2. 添加数据库 298
10.3.4.2.3. 管理已添加的数据库 299
10.3.4.3. 数据库详细信息 299
10.3.4.3.1. 概况（单库） 299
10.3.4.3.2. 风险 300
10.3.4.3.2.1. 查看风险统计结果 300
10.3.4.3.2.2. 查看风险命中记录 301
10.3.4.3.2.3. 检索风险语句 302
10.3.4.3.2.4. 查看风险语句模板 303
10.3.4.3.3. 语句 304
10.3.4.3.3.1. 查看SQL统计 304
10.3.4.3.3.2. 检索SQL语句 304
10.3.4.3.3.3. 检索语句模板 306
10.3.4.3.3.4. 查看执行失败的SQL语句 307
10.3.4.3.3.5. 查看TopSQL语句 308
10.3.4.3.3.6. 查看新型语句 309
10.3.4.3.3.7. 分析访问源 310

10.3.4.3.4. 会话 310
10.3.4.3.4.1. 查看会话统计 310
10.3.4.3.4.2. 检索会话信息 311
10.3.4.3.4.3. 查看登录失败会话 312
10.3.4.3.4.4. 查看活跃会话 312
10.3.4.3.5. 报表（单库） 313
10.3.4.3.5.1. 查看报表（单库） 313
10.3.4.3.5.2. 设置报表预存 315
10.3.4.3.5.3. 管理定时推送任务（单库） 316
10.3.4.3.6. 规则（单库） 317
10.3.4.3.6.1. 设置漏洞攻击规则 317
10.3.4.3.6.2. 设置语句规则 318
10.3.4.4. 报表 319
10.3.4.4.1. 查看报表 319
10.3.4.4.2. 管理定时推送任务 320
10.3.4.5. 系统告警信息 321
10.3.4.5.1. 查看系统告警信息 321
10.3.4.5.2. 配置系统告警 322
10.3.4.6. 配置 322
10.3.4.6.1. 用户管理 322
10.3.4.6.2. 角色管理 322
10.3.4.6.3. IP名称管理 323
10.3.4.7. 维护 324
10.3.4.7.1. 数据备份恢复 324
10.3.4.7.1.1. 设置自动备份 324
10.3.4.7.1.2. 手动备份与恢复 324
10.3.4.7.1.3. 查询备份清单 325
10.3.4.7.2. 自动清理告警与数据 325

10.3.4.7.3. 引擎管理 326
10.3.5. 审计管理员指南 327
10.3.5.1. 查看系统操作日志 327
10.4. 敏感数据保护 328
10.4.1. 敏感数据保护概览 328
10.4.2. 数据资产授权 329
10.4.2.1. 数据资产授权 329
10.4.2.2. 授权账密管理 341
10.4.3. 敏感数据发现 342
10.4.3.1. 敏感数据总览 342
10.4.3.2. 查看敏感数据资产 343
10.4.3.3. 搜索敏感数据 347
10.4.3.4. 识别任务监控 348
10.4.3.5. 识别规则 349
10.4.3.5.1. 查看识别规则 349
10.4.3.5.2. 管理识别模型 350
10.4.3.5.3. 管理模板 353
10.4.3.5.4. 设置风险级别 355
10.4.4. 云原生数据审计 356
10.4.4.1. 审计概览 356
10.4.4.2. 原始日志 361
10.4.4.3. 会话信息 366
10.4.4.4. 异常告警 367
10.4.4.5. 审计规则 368
10.4.4.5.1. 创建自定义规则 368
10.4.4.5.2. 查看内置规则 370
10.4.5. 数据权限 371
10.4.5.1. 查看权限统计 372

10.4.5.2. 检索权限 372
10.4.6. 数据流转监控 373
10.4.6.1. 查看DataHub 373
10.4.7. 数据脱敏 375
10.4.7.1. 新增静态脱敏任务 375
10.4.7.2. 查看动态脱敏API调用信息 379
10.4.7.3. 新增脱敏模板 379
10.4.7.4. 配置脱敏算法 382
10.4.7.5. 提取水印 387
10.4.8. 报表中心 388
10.4.8.1. 综合分析报告 388
10.4.8.2. 等保参考分析报表 389
10.4.9. 新增使用授权 390
10.5. 数据梳理 391
10.5.1. 快速部署指南 391
10.5.1.1. 部署数据梳理系统 391
10.5.1.2. 配置自定义IP 392
10.5.1.3. 登录数据梳理系统（云盾安全中心登录） 393
10.5.1.4. 导入许可证 393
10.5.2. 数据源管理 394
10.5.2.1. 创建数据库发现任务 394
10.5.2.2. 执行数据库发现任务 395
10.5.2.3. 管理数据库发现任务 395
10.5.2.4. 添加数据源 396
10.5.2.5. 查询数据源 397
10.5.3. 敏感数据任务管理 397
10.5.3.1. 自定义发现规则 397
10.5.3.2. 创建敏感数据任务 398

10.5.3.3. 执行敏感数据任务（单任务） 399
10.5.3.4. 批量执行任务 399
10.5.3.5. 查看敏感数据任务结果 400
10.5.4. 权限梳理任务管理 400
10.5.4.1. 创建权限梳理任务 400
10.5.4.2. 执行权限梳理任务（单任务） 401
10.5.4.3. 批量执行任务 401
10.5.4.4. 查看权限梳理任务结果 401
10.6. 数据发现与脱敏 402
10.6.1. 快速部署指南 402
10.6.1.1. 部署数据发现和脱敏系统 402
10.6.1.2. 配置自定义IP 403
10.6.1.3. 登录数据发现与脱敏系统 404
10.6.1.4. 数据脱敏系统界面 405
10.6.2. 使用指南 405
10.6.2.1. 数据源管理 406
10.6.2.1.1. 数据库 406
10.6.2.1.1.1. 添加数据库 406
10.6.2.1.1.2. 修改数据库 407
10.6.2.1.1.3. 删除数据库 408
10.6.2.1.1.4. 查询数据库 408
10.6.2.1.2. 文件源 408
10.6.2.1.2.1. 添加文件源 408
10.6.2.1.2.2. 添加文件 409
10.6.2.1.2.3. 修改文件信息 410
10.6.2.1.2.4. 删除文件 410
10.6.2.1.2.5. 修改文件源 410
10.6.2.1.2.6. 删除文件源 411

10.6.2.1.2.7. 查询文件源 411
10.6.2.2. 数据发现 411
10.6.2.2.1. 发现任务 411
10.6.2.2.1.1. 数据库发现任务 411
10.6.2.2.1.2. 文件发现任务 415
10.6.2.2.1.3. 查询发现任务 423
10.6.2.2.2. 敏感字段梳理 423
10.6.2.2.2.1. 添加敏感数据源 423
10.6.2.2.2.2. 核实敏感数据 424
10.6.2.2.2.3. 设置为非敏感数据 425
10.6.2.2.2.4. 修正敏感数据 426
10.6.2.2.2.5. 查询敏感数据 427
10.6.2.2.3. 敏感文件梳理 427
10.6.2.2.3.1. 核实敏感数据 427
10.6.2.2.3.2. 设置为非敏感数据 428
10.6.2.2.3.3. 修正敏感数据 429
10.6.2.2.3.4. 查询敏感数据 430
10.6.2.2.4. 发现规则 430
10.6.2.2.4.1. 查看发现规则 430
10.6.2.2.4.2. 添加自定义发现规则 431
10.6.2.3. 数据脱敏 431
10.6.2.3.1. 数据子集 431
10.6.2.3.1.1. 添加数据子集 431
10.6.2.3.1.2. 编辑数据子集 433
10.6.2.3.1.3. 删除数据子集 434
10.6.2.3.2. 数据关系 435
10.6.2.3.2.1. 查看数据关系 435
10.6.2.3.3. 脱敏方案 436

10.6.2.3.3.1. 添加数据库脱敏方案 436
10.6.2.3.3.2. 添加文件脱敏方案 438
10.6.2.3.3.3. 修改脱敏方案 440
10.6.2.3.3.4. 删除脱敏方案 441
10.6.2.3.4. 脱敏任务 442
10.6.2.3.4.1. 数据库脱敏任务 442
10.6.2.3.4.2. 文件脱敏任务 448
10.6.2.3.4.3. 查询脱敏任务 455
10.6.2.3.5. 脱敏算法 455
10.6.2.3.5.1. 查看脱敏算法 455
10.6.2.3.5.2. 添加自定义脱敏算法 456
10.7. 加密服务 456
10.7.1. 概述 456
10.7.2. 快速入门 457
10.7.2.1. 使用流程 457
10.7.2.2. 创建和配置加密实例 458
10.7.2.3. 注册管理员UKEY 458
10.7.2.4. 登录VsmManager管理工具 460
10.7.2.5. 执行原始初始化 460
10.7.2.6. 授权操作 465
10.7.2.7. 生成密钥 467
10.7.2.8. 配置主机端口属性 468
10.7.2.9. 签发应用许可 469
10.7.2.10. 配置TACSP 470
10.7.2.11. 配置密文通讯 473
10.7.2.12. 创建Demo实例 474
10.7.3. 加密实例管理 477
10.7.3.1. 创建加密实例 477

10.7.3.2. 配置加密实例 477
10.7.3.3. 释放加密实例 478
10.7.4. 密码机管理 478
10.7.4.1. 系统管理 478
10.7.4.1.1. 注册管理员UKEY 478
10.7.4.1.2. 登录VsmManager管理工具 479
10.7.4.2. 密钥管理 480
10.7.4.2.1. 执行原始初始化 480
10.7.4.2.2. 执行恢复初始化 485
10.7.4.2.3. 执行出厂初始化 486
10.7.4.2.4. 获取DMK校验值 487
10.7.4.2.5. 备份DMK 487
10.7.4.2.6. 对称密钥管理 488
10.7.4.2.6.1. 产生随机密钥 488
10.7.4.2.6.2. 成份合成密钥 490
10.7.4.2.6.3. 删除密钥 492
10.7.4.2.6.4. 清除全部密钥 493
10.7.4.2.6.5. 导出列表信息 494
10.7.4.2.6.6. ZMK保护导出 495
10.7.4.2.6.7. ZMK保护导入 497
10.7.4.2.7. 非对称密钥管理 498
10.7.4.2.7.1. 产生随机密钥 498
10.7.4.2.7.2. 删除密钥 500
10.7.4.2.7.3. 清除全部密钥 501
10.7.4.2.7.4. 导出列表信息 501
10.7.4.2.7.5. 生成证书请求 502
10.7.4.2.7.6. 导入私钥文件 503
10.7.4.2.8. 备份与恢复 504

10.7.4.2.8.1. 备份密钥 504
10.7.4.2.8.2. 恢复密钥 507
10.7.4.3. 设备管理 507
10.7.4.3.1. 配置主机端口属性 507
10.7.4.3.2. 配置设备时间 508
10.7.4.3.3. 授权管理 509
10.7.4.3.3.1. 授权操作 509
10.7.4.3.3.2. 获取授权状态 510
10.7.4.3.3.3. 取消授权 511
10.7.4.3.3.4. 签发应用许可 512
10.7.4.3.3.5. 管理应用许可 512
10.7.4.3.4. UKEY管理 513
10.7.4.3.4.1. 概述 513
10.7.4.3.4.2. 添加管理员 514
10.7.4.3.4.3. 注销管理员 514
10.7.4.3.4.4. 查询已注册的管理员UKEY信息 515
10.7.4.3.4.5. 获取UKEY详细信息 516
10.7.4.3.4.6. 更改UKEY信息 516
10.7.4.3.4.7. 更改UKEY口令 517
10.7.4.3.4.8. 格式化UKEY 518
10.7.4.3.5. 设备诊断维护 519
10.7.4.3.5.1. 导出日志 519
10.7.4.3.5.2. 清除日志 520
10.7.4.3.5.3. 查看设备基础信息 520
10.7.4.3.5.4. 设备自检 520
10.7.4.3.5.5. 查看主机服务状态 521
10.7.4.3.5.6. 查看设备资源信息 521
10.7.5. TACSP管理 521

10.7.5.1. 配置TACSP 521
10.7.5.2. 配置密文通讯 524
10.7.5.3. 启动TACSP 525
10.7.5.4. 重启TACSP 526
10.7.5.5. 停止TACSP 526
10.7.5.6. 设置TACSP日志级别 526
10.7.5.7. 停止连接密码机 526
10.7.5.8. 启动连接密码机 527
10.7.6. 调用加密实例 527
10.7.6.1. 创建Demo实例 527
10.7.6.2. Demo实例说明 529
10.8. 堡垒机 531
10.8.1. 概述 531
10.8.2. 快速部署指南 531
10.8.2.1. 部署堡垒机系统 531
10.8.2.2. 配置自定义IP 532
10.8.2.3. 登录云盾堡垒机（云盾安全中心登录） 533
10.8.2.4. 登录云盾堡垒机（一般Web方式登录） 534
10.8.2.5. 导入许可证 535
10.8.3. 超级管理员快速配置指南 536
10.8.3.1. 用户管理 536
10.8.3.1.1. 手工新建用户 536
10.8.3.1.2. 批量导入用户 538
10.8.3.1.3. 管理用户 539
10.8.3.1.4. 配置用户信息 539
10.8.3.2. 用户组管理 541
10.8.3.2.1. 新建用户组 541
10.8.3.2.2. 管理用户组 541

10.8.3.2.3. 对用户进行分组 542
10.8.3.3. 主机管理 543
10.8.3.3.1. 手工新建主机 543
10.8.3.3.2. 批量导入主机 543
10.8.3.3.3. 管理主机信息 544
10.8.3.3.4. 设置主机帐户 545
10.8.3.3.5. 管理主机配置 546
10.8.3.4. 主机组管理 547
10.8.3.4.1. 新建主机组 547
10.8.3.4.2. 管理主机组 548
10.8.3.4.3. 对主机进行分组 548
10.8.3.5. 帐户组管理 549
10.8.3.5.1. 新建帐户组 549
10.8.3.5.2. 管理帐户组信息 550
10.8.3.6. 运维授权 550
10.8.3.6.1. 运维规则概述 550
10.8.3.6.2. 新建运维规则 550
10.8.3.6.3. 管理运维规则 552
10.8.3.7. 未授权运维审核 555
10.8.3.7.1. 未授权登录审核 555
10.8.3.7.2. 审批运维工单 555
10.8.3.8. 实时监控 556
10.8.4. 运维人员操作指南 557
10.8.4.1. 下载运维工具 557
10.8.4.2. Web方式运维（适用于Windows） 558
10.8.4.2.1. 安装单点登录器 558
10.8.4.2.2. 指定运维工具 558
10.8.4.2.3. 通过SSH协议登录主机进行运维 559

10.8.4.2.4. 通过RDP协议登录主机进行运维 560
10.8.4.2.5. 通过SFTP协议登录主机进行运维 561
10.8.4.2.6. 未授权登录主机进行运维 562
10.8.4.2.7. 运维审批申请 563
10.8.4.3. CS方式运维操作指南 563
10.8.4.3.1. 在苹果操作系统上运维 563
10.8.4.3.1.1. 准备工作 563
10.8.4.3.1.2. 通过命令行终端app的菜单方式登录目标主机进行... 564
10.8.4.3.1.3. 通过远程桌面连接app的菜单方式登录目标主机进... 565
10.8.4.3.2. 在Windows操作系统上运维 567
10.8.4.3.2.1. 准备工作 568
10.8.4.3.2.2. 通过SSH工具登录目标主机进行运维 568
10.8.4.3.2.3. 通过远程桌面连接工具的菜单方式登录目标主机进... 571
10.8.4.3.2.4. 通过WinSCP工具登录目标主机进行运维 574
10.8.4.3.2.5. 通过XFTP工具登录目标主机进行运维 575
10.8.4.4. 新建工单 577
10.8.5. 审计管理员操作指南 578
10.8.5.1. 审计规则 578
10.8.5.1.1. 添加审计规则 578
10.8.5.2. 会话审计 579
10.8.5.2.1. 搜索审计会话 579
10.8.5.2.2. 查看所有会话 580
10.8.5.2.3. 搜索事件 582
10.8.5.2.4. 查询事件 582
10.8.5.3. 运维报表 583
10.8.5.3.1. 按时间范围查看运维报表 583
10.8.5.3.2. 设置报表自动发送 584
10.8.6. 系统管理员操作指南 585

10.8.6.1. 网络设置 585
10.8.6.1.1. 配置网络信息 585
10.8.6.1.2. 配置Web 586
10.8.6.1.3. 配置静态路由 587
10.8.6.1.4. 配置SNMP 587
10.8.6.1.5. 配置IP源防护 588
10.8.6.2. 认证管理 588
10.8.6.2.1. 配置安全设置 588
10.8.6.2.2. 设置远程认证 589
10.8.6.2.3. 配置双因子认证 591
10.8.6.3. 系统配置 592
10.8.6.3.1. 配置运维管理 592
10.8.6.3.2. 配置告警信息 594
10.8.6.3.3. 配置语言和界面 594
10.8.6.3.4. 配置功能 595
10.8.6.3.5. 配置SSH KEY 595
10.8.6.4. 存储管理 595
10.8.6.4.1. 数据归档 595
10.8.6.4.2. 录像导出 597
10.8.6.4.3. 日志备份 598
10.8.6.5. 查看系统操作日志 598
10.8.6.6. 查看系统报表 599
10.8.6.7. 本机维护 601
10.8.6.7.1. 管理系统 601
10.8.6.7.2. 升级系统 601
10.8.6.7.3. 导入许可证 602
10.8.6.7.4. 查看资源监控信息 603
10.8.6.7.5. 备份还原系统配置 603

10.8.6.7.6. 推送和接收系统配置 604
10.8.6.7.7. 查看调试日志 605
10.8.6.7.8. 网络诊断 605
10.8.6.7.9. 系统诊断 605
10.8.6.7.10. 查看系统警报 606
10.8.6.7.11. 生成控制台SSH公钥 606
10.9. 堡垒机（New） 606
10.9.1. 创建和登录堡垒机 606
10.9.2. 管理员操作指南 608
10.9.2.1. 系统管理 608
10.9.2.1.1. 设置Web登录超时时间 608
10.9.2.1.2. 设置对外输出方式 609
10.9.2.2. 用户管理 615
10.9.2.2.1. 配置全局安全策略 615
10.9.2.2.2. 配置用户认证模式 616
10.9.2.2.3. 创建用户 619
10.9.2.2.4. 创建用户组 621
10.9.2.3. 主机管理 622
10.9.2.3.1. 创建主机账号 622
10.9.2.3.2. 创建主机的设备类型 623
10.9.2.3.3. 手动创建主机 624
10.9.2.3.4. 批量导入主机 626
10.9.2.3.5. 创建主机组 627
10.9.2.4. 运维管理 628
10.9.2.4.1. 配置全局运维策略 628
10.9.2.4.2. 配置访问授权 630
10.9.2.4.3. 配置指令授权（按对象授权） 634
10.9.2.4.4. 配置指令授权（按访问授权） 638

10.9.2.5. 资源管理 640
10.9.2.5.1. 创建服务器集合 640
10.9.2.5.2. 创建客户端集合 641
10.9.2.5.3. 创建指令集合 642
10.9.2.5.4. 创建审批策略 642
10.9.2.5.5. 创建事件告警 644
10.9.2.5.6. 创建密钥 645
10.9.2.6. 密码管理 646
10.9.2.6.1. 密码录入 646
10.9.2.6.2. 密码导出 648
10.9.2.6.3. 主机设定 648
10.9.2.6.4. 改密设定 650
10.9.2.6.5. 自动改密 652
10.9.2.6.6. 手工改密 655
10.9.2.7. 审计管理 655
10.9.2.7.1. 查看实时监控信息 655
10.9.2.8. 消息中心 656
10.9.2.8.1. 发送消息 656
10.9.2.8.2. 查看消息 657
10.9.3. 运维员操作指南 657
10.9.3.1. 登录堡垒机运维环境 657
10.9.3.2. 安装运维客户端 659
10.9.3.3. 通过Web方式运维 659
10.9.3.4. 通过客户端方式运维 660
10.10. 平台侧堡垒机 663
10.10.1. 概述 663
10.10.2. 工具下载 663
10.10.3. 管理员操作指南 664

10.10.3.1. 实时监控 664
10.10.3.2. 数据检索 665
10.10.3.3. 运维报表 665
10.10.3.4. 用户管理 666
10.10.3.4.1. 配置全局安全策略 666
10.10.3.4.2. 创建用户认证模式 667
10.10.3.4.3. 创建用户组及用户 668
10.10.3.5. 主机管理 670
10.10.3.5.1. 创建主机账号 670
10.10.3.5.2. 创建主机的访问协议 671
10.10.3.5.3. 创建主机组及主机 672
10.10.3.6. 运维管理 674
10.10.3.6.1. 配置全局运维策略 674
10.10.3.6.2. 配置访问授权 676
10.10.3.6.3. 配置指令授权（按对象授权） 680
10.10.3.6.4. 配置指令授权（按访问授权） 684
10.10.3.7. 资源管理 686
10.10.3.7.1. 创建账号 686
10.10.3.7.2. 创建客户端集合 686
10.10.3.7.3. 创建指令集合 687
10.10.3.7.4. 创建审批策略 688
10.10.3.7.5. 创建事件告警 689
10.10.3.7.6. 创建服务器集合 691
10.10.3.7.7. 创建密钥 692
10.10.3.8. 系统管理 693
10.10.3.8.1. 设置Web登录超时时间 693
10.10.3.8.2. 设置对外输出方式 693
10.10.3.9. 密码管理 697

10.10.3.9.1. 密码录入 697
10.10.3.9.2. 密码导出 699
10.10.3.9.3. 主机设定 699
10.10.3.9.4. 改密设定 701
10.10.3.9.5. 自动改密 702
10.10.3.9.6. 手工改密 705
10.10.3.10. 消息中心 706
10.10.3.10.1. 发送消息 706
10.10.3.10.2. 查看消息 707
10.10.4. 运维员操作指南 707
10.10.4.1. 登录堡垒机运维环境 707
10.10.4.2. 安装运维客户端 708
10.10.4.3. 通过Web方式运维 708
10.10.4.4. 通过客户端方式运维 709
10.11. 安全编排自动化响应 712
10.11.1. 事件调查 712
10.11.1.1. 案件管理 712
10.11.1.2. 任务列表 716
10.11.1.3. 响应动作 716
10.11.2. 自动化编排 718
10.11.2.1. 剧本管理 718
10.11.2.2. 组件列表管理 721
10.11.3. 知识管理 726
10.11.3.1. 情报管理 726
10.11.3.2. 名单库 729
10.11.4. 系统配置 734
10.11.4.1. 环境变量配置 734
10.11.4.2. 管理流式数据源 736

10.11.4.3. 管理第三方包 736
10.11.4.4. 剧本执行日志 737
10.12. 容器防护 739
10.12.1. 查看容器服务ACK应用 739
10.12.2. 查看ACR镜像 739
10.12.3. 镜像安全扫描 740
10.12.4. 入侵事件告警 741
10.12.5. 日志检索 742
11.云盾系统配置 743
11.1. 规则运营 743
11.1.1. 添加流量安全监控IPS规则 743
11.1.2. 管理云防火墙IPS规则 744
11.1.3. 添加流量安全监控IDS规则 744
11.1.4. 管理流量安全监控IDS规则 745
11.1.5. 自定义DDoS清洗策略和牵引阈值 746
11.1.6. 查看安骑士规则 746
11.2. 威胁情报 747
11.2.1. 查看总览 747
11.2.2. 查看IP搜索信息 748
11.2.3. 配置消费产品 749
11.3. 告警设置 750
11.3.1. 设置告警联系人 750
11.3.2. 设置告警通知 751
11.4. 升级中心 752
11.4.1. 升级中心概述 752
11.4.2. 自动检查更新并升级 752
11.4.3. 手动导入升级包并升级 753
11.4.4. 回滚规则库 754

11.4.5. 查看历史记录 754
11.4.6. 升级包下载 754
11.5. 全局设置 756
11.5.1. 流量采集网段设置 756
11.5.1.1. 添加流量采集网段 756
11.5.1.2. 管理流量采集网段 757
11.5.2. 区域设置 757
11.5.2.1. 添加区域网段 757
11.5.2.2. 管理区域网段 758
11.5.3. 配置白名单 759
11.5.4. 配置拦截策略 760
11.5.5. 一键封禁 760
11.5.6. 自定义IP地理位置设置 762
11.5.6.1. 添加自定义IP地理位置 762
11.5.6.2. 管理自定义IP地理位置 762
11.6. 系统监控 763
11.6.1. 配置云防火墙的引流网段 763
11.6.2. 系统巡检 763
11.7. 账号管理 764
11.7.1. 查看和修改专有云账号 764
11.7.2. 添加公共云账号 766
11.8. 安全监控 767

1.什么是云盾

专有云云盾是专有云的安全解决方案，从网络、服务器、应用、数据、安全管理和安全服务等多方面保护云上资产安全。

背景信息

传统IT服务使用的安全解决方案，是以检测技术为主的网络边界安全防护，通过防火墙、入侵防御等硬件安全产品将攻击者挡在网络边界之外。

云计算具有低成本、按需灵活配置和高资源利用率等优势。随着云计算的发展，越来越多的企业和组织从传统IT服务转向云计算服务。云计算兴起之后，网络边界的概念变得越来越模糊，传统的安全解决方案无法很好的保护云上资产的安全。

专有云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、主机层等多个方面为专有云提供一体化的安全解决方案。

完整的安全解决方案

安全域	服务名称	安全设计
安全运营	态势感知	通过态势感知服务实现流量监控、整体安全监控，实现安全审计与集中管控。
	漏洞扫描	结合人工智能技术帮助企业及时发现安全风险的智能安全产品。
	安全自动编排响应SOAR	通过SOAR安全自动化编排，将安全事件运营自动化、流程化，提升安全响应速度。
	云安全管理中心SOC	云原生的一体化安全运营中心，适用于云环境的整体安全运营管理，可以构建云环境风险预测发现、防御控制、检测分析、响应管理的闭环安全运营体系。
主机安全	安骑士（主机安全）	通过安骑士服务实现对ECS的入侵防范和恶意代码防范。
	物理机主机安全	通过主机入侵检测服务实现对物理机的入侵防范。
	容器防护	通过容器防护实现对阿里云上容器及其运行环境的入侵防范。
应用安全	Web应用防火墙	通过Web应用防火墙防护恶意应用攻击，保障移动、PC等互联网用户的接入安全。
网络安全	DDoS防护	通过DDoS防护服务提供网络链路可用性保证，提升业务连续性。
	云防火墙	通过云防火墙服务，统一管理互联网到业务以及业务之间的访问控制策略（东西向和南北向）。
	网络流量检测与响应	通过多种威胁检测引擎和威胁情报，检测互联网边界和内网边界流量中的网络攻击行为，并对攻击行为进行响应。
	数据库审计	通过数据库审计服务实现对数据库的审计功能。
	敏感数据保护	通过敏感数据保护服务帮助您防止数据泄露和满足合规要求。

安全域	服务名称	安全设计
数据安全	数据发现与脱敏	通过数据发现与脱敏服务帮助您对敏感数据进行脱敏，防止数据泄露和满足合规要求。
	数据梳理	通过数据梳理服务帮助您发现敏感数据，防止数据泄露和满足合规要求。
	加密服务	通过加密服务满足金融、互联网等行业加密需求，保障业务数据隐私安全。
内容安全	内容安全	通过内容安全服务帮助用户降低内容违规风险。
运维审计	安全审计	通过安全审计服务汇总和分析日志，以便安全审计员及时发现并消除安全隐患。
	堡垒机	通过堡垒机管理运维ECS，实现云上服务器的操作运维审计和账号权限管理。
安全服务	安全运营驻场服务	帮助您更好地利用专有云产品及云盾安全产品的安全特性，为您建立和持续优化云安全防御体系，保障您的业务安全。

2.使用须知

在登录云盾控制台前，您需要确认本地PC符合以下配置。

本地PC需要满足如配置要求表中配置要求，才可以正常登录云盾控制台。

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 • 国密浏览器：Chrome内核69及以上的主流国密浏览器
操作系统	• Windows XP版本 • Windows 7及以上版本 • Mac系统

3.快速入门

3.1. 用户权限说明

本文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，请参见云盾默认角色。

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，请参见*Apsara Uni-manager运营控制台用户指南*中**创建用户**。

3.2. 登录云盾安全中心

本文介绍了如何登录到云盾安全中心。

前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的服务域名地址，按回车键。
2. 输入正确的用户名及密码。

   请向运营管理员获取登录控制台的用户名和密码。

> **说明** 首次登录Apsara Uni-manager运营控制台时，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，密码长度必须为10~32位，且至少包含以下两种类型：
>
> - 英文大写或小写字母（A~Z、a~z）
> - 阿拉伯数字（0~9）
> - 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（$）、百分号（%）等）

3. 单击**账号登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
   - 管理员强制开启MFA后的首次登录：
     a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
     b. 按照步骤2重新输入账号和密码，单击**账号登录**。
     c. 输入6位MFA码后单击**认证**。
   - 您已开启并绑定MFA：

     输入6位MFA码后单击**认证**。

     > **说明** 绑定并开启MFA的操作请参见*Apsara Uni-manager运营控制台用户指南*中的章节*绑定并开启虚拟MFA设备*。
5. 在页面顶部的导航栏中，选择**安全 > 云盾**。
6. 在**云盾控制台**页面，选择**地域**。
7. 单击**角色授权访问**，进入云盾安全中心。

4.态势感知

4.1. 概述

本文介绍了态势感知的基本概念。

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，评估威胁程度。

态势感知包含以下内容：

- 总览：展现安全的整体态势和安全大屏相关信息。
- 安全告警：展现业务系统中已经发生的安全事件。
- 攻击分析：展现当前系统面临的应用攻击和暴力破解事件。
- 云产品检查：检查云产品的安全配置是否存在安全隐患。
- 应用白名单：通过AI智能学习将需要重点防御的服务器加入到白名单中，通过检测白名单中指定的应用程序区分可信、可疑和恶意程序，防止未经白名单授权的程序运行。
- 资产中心：管理专有云环境中的服务器和云产品。
- 漏洞扫描：展现系统中存在的漏洞和缺陷。
- 安全报告：配置专有云平台安全报告任务。

4.2. 总览

4.2.1. 查看安全总览信息

本文介绍了如何查看专有云平台的安全统计、攻击趋势和网络流量信息。

背景信息

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。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. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**总览**。
4. 在**安全总览**页签下查看专有云平台安全的总览情况。



安全总览页面区域说明表

功能	说明
安全评分	资产的安全分值以及发现资产安全风险数量。
资产状态	查看资产总数、未在防护范围内的服务器数量、关机服务器数量，以及存在风险服务器的统计数据。
安全检测及防御能力	提供近15天精准防御数、近15天网页防篡改数、病毒库更新时间、系统漏洞扫描时间，帮助您实时掌握安全防御情况，了解资产安全状态。
威胁统计	查看待处理告警、待修复漏洞、基线问题的数量及攻击次数。
云平台配置风险	检测到的云产品基线配置存在的风险。
安全运营	展示近15天已处理的告警、漏洞、基线配置数量柱状图和趋势图。

4.2.2. 查看安全大屏

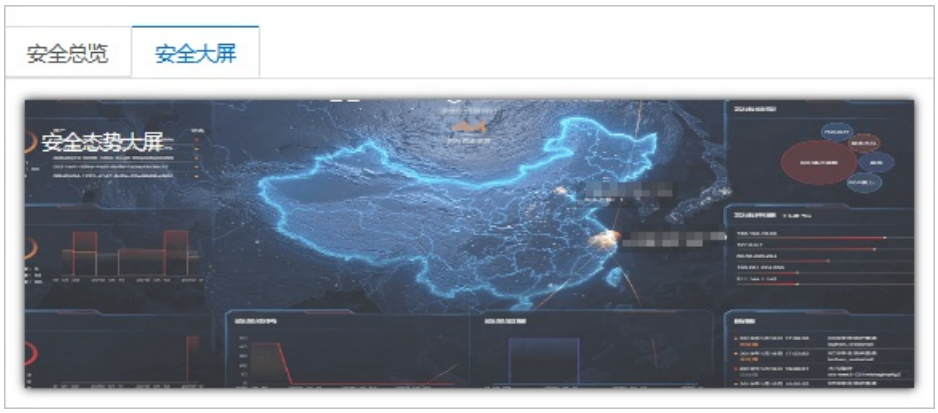
态势感知安全大屏可从您资产的当前安全情况、外部攻击情况、威胁情况三个维度为您全面展现当前资产的网络安全态势。

背景信息

安全大屏将安全攻防数据转化并呈现到安全大屏上，秒级更新实时数据，可实时展现资产、漏洞、基线情况，帮助您一眼看清资产当前的安全状态；实时展现攻击来源、攻击分布、明确攻击者来源及攻击情况，帮助您建立安全防线，提升资产的整体防御能力；实时为您呈现告警概览并及时响应，帮助您构建实时威胁感知能力，将入侵损失降低到最小。

查看安全大屏信息

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**总览**。
4. 在**总览**页面，单击**安全大屏**页签。



5. 在**安全态势大屏**中，单击**直接访问**。

   查看安全大屏信息。



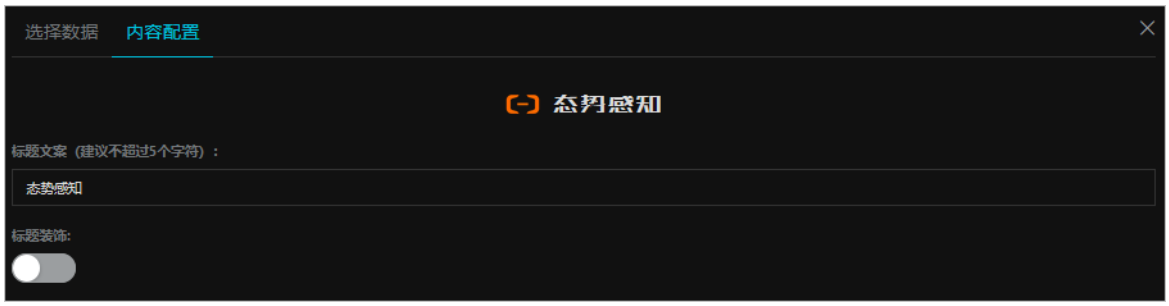
- 攻击地域地图：态势感知安全大屏正中间位置以动态方式展示了攻击地域地图，显示检测到资产受到的攻击来源方向、攻击来源地区、攻击来源IP地址和攻击次数等信息。
- 漏洞：展示了资产中漏洞的总数量、不同危险等级漏洞的环形占比图、需处理的漏洞类型和对应的数量、最近7天不同风险等级的漏洞的数据统计柱状图。
- 资产：展示了云盾检测到的资产统计信息。
- 基线：展示了资产中基线风险项的总数量，高危、中危、低危基线风险项数量，及最近7天不同危险等级的基线风险项的数据统计柱状图。
- 安全态势：展示了最近7天、15天或30天安全评分的趋势图。当天统计数据为实时数据。
- 攻击来源TOP5：展示了最近24小时内服务器受到的攻击次数排名前5的攻击来源IP地址及其发起的攻击次数。
- 告警：展示了最近24小时内未处理的、已处理、排名前5的高风险告警列表，包括告警事件发生的时

间、事件名称和服务器名称。

- 最高风险资产：展示了最近24小时内服务器受到的攻击次数排名前5的服务器IP地址及被攻击次数。
- 云平台最佳实践：展示了云平台配置检查功能实时检测出的项目信息。

自定义安全大屏展示内容

1. 在**安全大屏**页面，单击右上角图标。
2. 在**内容配置**页签，配置需要在大屏上显示的**标题文案**。



3. （可选）单击**选择数据**页签，并完成数据配置。

   选中需要在大屏上实时展示的数据类型。您可以选中**全部**或单个数据分类。



4. 单击**保存设置**。

大屏内容设置完成后，您可以在大屏页面看到根据您自定义设置展示的大屏内容。

自定义大屏场景

为满足不同业务领域展示不同场景数据的需要，安全大屏支持自定义场景。您可以根据业务的需要自定义多个不同的大屏场景。

1. 在**安全大屏**页面，单击右上角图标。
2. 在**场景列表**页面，单击**新增场景**。



3. 在**内容配置**页签，配置需要在大屏上显示的**标题文案**。
4. 单击**选择数据**页签并完成数据配置。

   选中需要在大屏上实时展示的数据类型。您可以选中**全部**或单个数据分类。



5. 单击**保存设置**。

新增场景完成后，会默认启用该场景，您可以在大屏页面看到该场景的相关数据展示。

如果您需要展示其它场景，可在**场景列表**页面定位到需要展示的场景并单击**立即启用**。



> **说明** 安全大屏自定义场景不限数量。

4.3. 安全告警

4.3.1. 查看安全告警

您可以通过安全告警页面查看安全告警事件。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**安全告警**。
4. （可选）设置安全告警信息的过滤条件。

   > **说明** 如果您想查看所有告警信息，则不需要进行过滤。

过滤条件	说明
告警等级	选择需要查看的安全告警等级，可多选，支持以下级别： ○ 紧急 ○ 可疑 ○ 提醒
告警处理状态	选择安全告警的处理状态，支持以下状态： ○ 待处理告警 ○ 已处理
告警类型	选择安全告警的类型，支持选择**全部告警类型**和具体告警类型。
影响资产分组	选择安全告警中受影响的资产分组，支持选择**全部资产分组**和具体资产分组。
告警名称、资产搜索	通过输入告警名称或受影响资产的关键字，搜索相关结果。

5. 在安全告警列表中，查看安全告警及其详细信息。

4.3.2. 管理文件隔离箱

系统对检测到的威胁文件进行隔离处理。被成功隔离的文件可在30天内进行一键恢复，过期后系统将自动清除被隔离文件。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**安全告警**。
4. 在**安全告警处理**页面右上角，单击**文件隔离箱**。
5. 在**文件隔离箱**面板，查看被隔离的文件主机地址、文件路径、状态和操作时间等信息。



6. （可选）在误报后被隔离的文件**操作**栏，单击**恢复**。

   注意 在进行恢复操作前，请确认该威胁文件为误报。

   通过恢复操作，可以将指定的被隔离文件从文件隔离箱中恢复。恢复的文件将重新回到安全告警列表中。

4.3.3. 安全告警设置

安全告警设置支持手动维护常用登录地和Web目录。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**安全告警**。
4. 在**安全告警**页面右上角，单击**安全告警设置**。

   在**安全告警设置**面板，您可以进行以下操作：

   - **添加常用登录地**
     a. 单击**常用登录地**右侧的**管理**按钮。



b. 在**常用登录地**页签，选择要添加的常用登录地，然后选择添加应用的服务器。



c. 单击**确定**，完成添加。

云盾态势感知支持**编辑**和**删除**已成功添加的常用登录地。

- 单击目标常用登录地右侧的**编辑**，修改该登录地的生效服务器。
- 单击目标常用登录地右侧的**删除**，删除该常用登录地配置。

- **配置高级登录报警**

> **说明** 配置高级登录告警，可进一步指定合法的登录IP、时间段和账号。配置完成后，态势感知会对非指定的登录情形进行告警。以下功能的操作类似**常用登录地**配置，可参考上文进行**添加**、**编辑**、**删除**。

- 单击**常用登录IP**右侧的切换开关，开启或关闭登录IP报警，开启后通过非常用IP登录会触发报警。



- 单击**常用登录时间**右侧的切换开关，开启或关闭登录时间报警，开启后在非常用时间登录会触发报警。



- 单击**常用账号**右侧的切换开关，开启或关闭登录账号报警，开启后使用非指定账号登录会触发报警。



- **Web目录定义**

  云盾会自动检测服务器资产中的Web目录，并进行动态检测和静态扫描；您也可以手动添加服务器中的其它Web目录进行检测扫描。



  a. 单击**Web目录定义**右侧的**添加**。

  b. 输入一个合法的Web路径，然后选择生效服务器，该路径所对应的Web目录会被添加到检测列表中。

  > **说明** 直接添加root目录会影响性能、效率，因此不支持直接添加。

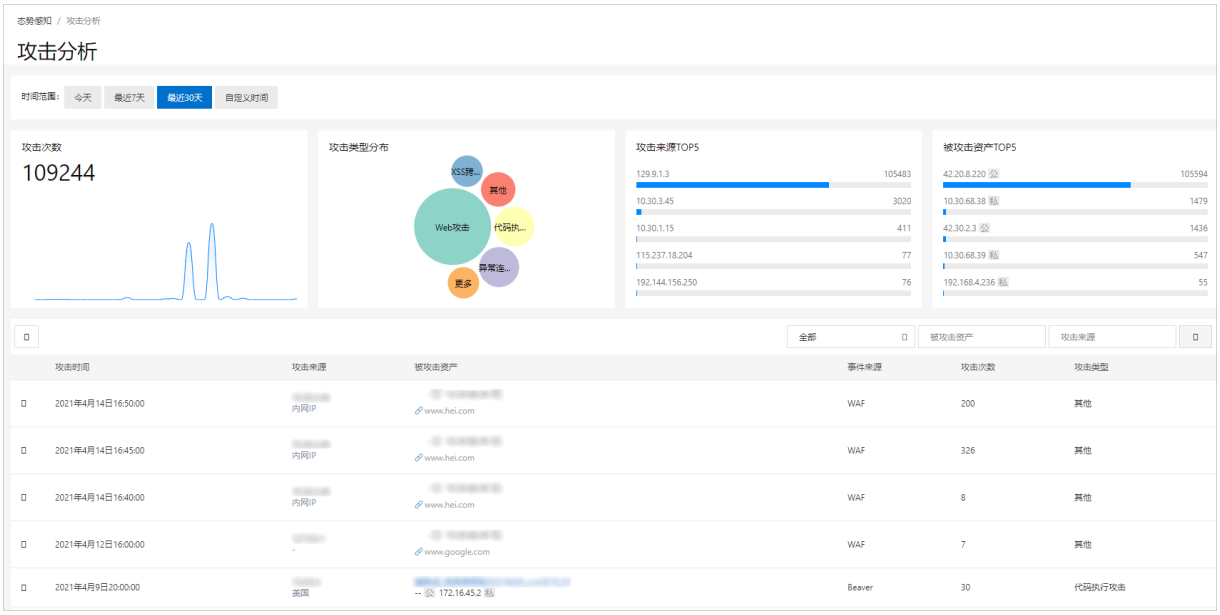
  c. 单击**确定**，完成添加。

4.4. 攻击分析

本文介绍了攻击分析的统计信息，包括攻击次数、攻击类型分布、攻击来源TOP 5、被攻击资产TOP 5和攻击详情列表。

背景信息

攻击分析基于云盾控制台的安全防护能力，提供基础攻击检测和防护。建议您根据自身业务需求，可考虑从防火墙和业务安全方面构建更精细化的纵深防护体系。



在**攻击分析**页面，您可以设置时间范围查看以下攻击分析结果。您可以快速查看当天、最近7天或最近15天内的攻击分析结果，也可以选择**自定义时间**，查看最近30天内任意时间范围的攻击分析结果。

- **攻击次数**：指定时间范围内资产被攻击的总次数。
- **攻击类型分布**：攻击类型和对应的攻击次数。
- **攻击来源TOP5**：攻击次数排名前5位的攻击来源IP地址。
- **被攻击资产TOP5**：攻击次数排名前5位的被攻击资产。
- **攻击详情列表**：所有攻击事件的详细信息，包含攻击发生的时间、攻击来源IP地址、被攻击的资产信息、攻击次数和攻击类型等信息。

> **说明** 攻击详情列表展示攻击数据上限为10000条。如需查看更多数据可切换**时间范围**查看指定时间范围内的全部攻击数据。

攻击详情参数表

内容	描述
攻击时间	攻击发生的时间。
攻击来源	发起攻击的源IP地址。
被攻击资产	被攻击资产的名称和公网、私网IP地址。

内容	描述
攻击次数	攻击发生的次数。
攻击类型	攻击事件的类型，如SSH暴力破解、代码执行等。

- 搜索查看攻击事件

  您可通过攻击详情列表上方搜索条件，筛选指定的攻击类型、被攻击资产、攻击来源和端口，搜索目标的攻击事件并查看其详细信息。



- 查看被攻击资产信息

  将鼠标悬浮到**被攻击资产**名称处可查看该资产的基本信息。



- 导出攻击事件列表

  单击攻击事件列表左上方的 图标，将云盾控制台检测出的攻击事件统一导出并保存到本地。导出的文件为Excel格式。

4.5. 云产品检查

4.5.1. 云产品检查概述

云盾安全中心态势感知支持云产品检查功能，检查您云产品的安全配置是否存在安全隐患。本文介绍了云产品检查功能的特性和检查项信息。

背景信息

云产品检查为您提供网络访问控制、数据安全两种类型的检查，帮助您及时发现云产品配置风险并提供相应的修复方案。

您可以在云盾安全中心态势感知的**云产品检查**页面，查看**已启用检查项**数。



云产品检查项列表

云产品检查项如下所示：

检查类型	支持的检查项	说明
数据安全	PolarDB-备份设置	检查云数据库PolarDB是否开启了自动备份功能。数据库定期备份有利于提升数据库安全，在出现数据库异常时可以根据历史备份信息进行恢复。云数据库PolarDB提供了自动备份策略，建议您保持开启，确保每天备份一次。
	容器镜像服务-仓库权限设置	检查容器镜像服务的仓库是否设置为私有。容器镜像服务的仓库分为公有仓库和私有仓库，公有仓库允许所有互联网用户匿名下载。如果镜像内部有敏感信息，建议设置为私有；如果没有，可以忽略该条告警。
	OSS-Bucket服务端加密	检测OSS Bucket是否开启数据加密功能。OSS提供服务器端加密功能，对持久化在OSS上的数据进行加密保护，建议您对敏感类型数据开启。
	OSS敏感文件泄露	检测OSS敏感文件是否有设置访问权限。
	RDS-跨地域备份	检测RDS数据实例是否开启跨地域备份功能。RDS为MySQL提供跨地域备份功能，可以自动将本地备份文件复制到另一个地域的OSS上，跨地域的数据备份能够有效的实现异地容灾。建议您开启跨地域备份。
	Redis-备份设置	检测Redis数据库实例是否开启了数据备份功能。
	MongoDB-SSL开启	检测MongoDB数据库是否开启SSL加密。为提高MongoDB数据库数据链路的安全性，建议您启用SSL加密。
	MongoDB-备份设置	检测云数据库MongoDB是否开启自动备份功能。数据库定期备份有利于提升数据库安全，在出现数据库异常时可以根据历史备份信息进行恢复。云数据库MongoDB提供了自动备份策略，建议您保持开启，确保每天备份一次。
	ECS-存储加密	检测ECS主机磁盘是否开启了加密功能。
	ECS-自动快照策略	检测ECS磁盘是否开启自动快照功能。自动快照可以提升ECS主机的数据安全，实现容灾备份。
	OSS-Bucket权限设置	检测OSS Bucket权限是否设置成了*私有*。
	OSS-日志记录配置	检测OSS是否有开启日志记录功能。
	OSS-跨区域复制配置	检测OSS是否有开启跨区域复制功能。

检查类型	支持的检查项	说明
	RDS-数据库安全策略	检测RDS数据库是否开启了SQL审计功能、SSL加密传输功能和透明数据库加密功能。
	RDS-开启数据库备份	检测RDS数据库实例是否开启了数据备份功能。
	SSL证书-有效期检查	检测SSL证书是否超出有效期。如果证书过期，您将无法继续使用SSL证书服务。
网络访问控制	ECS-安全组策略	检测ECS访问策略。建议安全组最小粒度开放访问策略，仅对必须全网开放的服务才开启0.0.0.0/0，例如80、443、22、3389端口。
	OSS-Bucket防盗链配置	检测OSS-Bucket是否开启防盗链功能。OSS防盗链功能通过检查Referer，进行白名单限制，可以用于防止他人盗用OSS数据，建议您开启。
	VPC-DNAT管理端口开放	检测端口是否映射到公网。建议VPC NAT网关创建DNAT规则时不要将内部管理端口映射在公网，例如所有端口都映射，或者22、3389、1433、3306等重要端口。
	云盾-高防回源配置检查	检测DDoS高防服务是否有配置仅允许WAF回源IP地址访问。使用DDoS高防服务或Web应用防火墙后，需要对后端服务器真实IP地址进行隐藏，避免攻击者绕过高防或WAF直接攻击云主机。
	云盾-WAF回源配置	检测WAF（Web应用防火墙）服务是否配置仅允许WAF回源IP地址访问。使用DDoS高防服务或Web应用防火墙后，需要对后端服务器真实IP地址进行隐藏，避免攻击者绕过高防或WAF直接攻击云主机。
	SLB-白名单配置	检测SLB负载均衡实例访问控制配置，http、https服务是否启用了访问控制，并且是否有开放0.0.0.0/0。
	SLB-高危端口暴露	检测SLB是否开启了转发非必要的公共服务端口。
	RDS-白名单配置	检测RDS的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。
	Redis-白名单配置	检测Redis的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。
	分析型数据库PostgreSQL版-白名单配置	检测PostgreSQL的访问控制策略是否有0.0.0.0/0（任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。
	PolarDB-白名单配置	检测云数据库PolarDB的访问控制策略是否开放公网访问且有 `0.0.0.0/0` （任意IP）的配置，不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。

检查类型	支持的检查项	说明
	MongoDB-白名单配置	检测MongoDB的访问控制策略是否有 `0.0.0.0/0` （任意IP）或为空的配置。不建议数据库类服务直接对公网开放，需要限定访问范围为指定IP访问。

4.5.2. 执行云产品检查

云盾安全中心态势感知的云产品检查功能支持检查您云产品中是否存在配置上的风险。本文介绍了如何在云盾安全中心对云产品执行即时手动检查，及设置检测周期进行周期性自动检查。

背景信息

云盾安全中心支持手动立即检查和周期性自动检查云平台配置是否存在风险。

- 手动检查：在**云平台配置检查**页面，执行**立即检查**，即时手动检查您云产品的配置是否存在风险。
- 周期性自动检查：云盾安全中心默认每隔1天在 `00:00:00~06:00:00` 自动检查云平台配置是否存在风险。您也可根据需要设置自定义的检测周期，定期检查云平台配置，帮助您及时发现并处理您的云产品配置风险。

手动检查

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**云产品检查**。
4. 在**云平台配置检查**页面，单击检查项列表上方的**立即检查**，对云产品配置进行全量检查，确定是否存在风险项以及影响的资产数量。

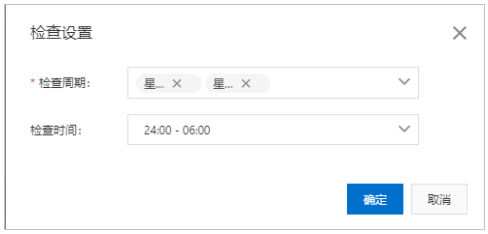


> **说明** 全量检查时，需要完成全部检查项的检查后才可以进行其他操作，请耐心等待。

完成检查后，检查项列表中按检查结果的严重等级由高风险到低风险进行排序。

自动检查

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**云产品检查**。
4. 在**云平台配置检查**页面右上角，单击**检查设置**。
5. 在**检查设置**对话框中，设置云产品配置项的**检查周期**和**检查时间**。



- **检查周期**：可选星期一至星期日，支持多选。
- **检查时间**：可选择 `24:00:00~06:00:00` 、 `06:00:00~12:00:00` 、 `12:00:00~18:00:00` 、 `18:00:00~24:00:00` 这4个时间段中的任意一个。

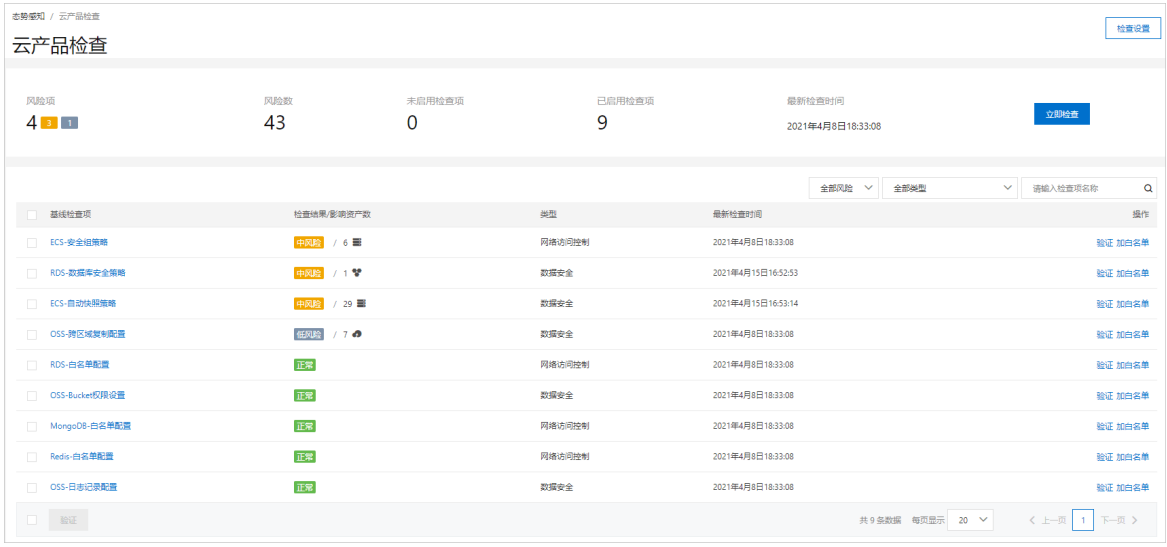
6. 单击**确定**。
   在选定时间段内，云盾安全中心会对所有检查项自动执行一次检查。

4.5.3. 查看和处理云产品检查结果

本文介绍了如何在云盾安全中心查看并处理云平台配置检查结果，具体包括检查项、检查项详情描述、可能产生的影响和处理建议。您可以在云平台配置检查页面集中处理检查出来的风险配置项。

查看云平台配置检查结果

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**云产品检查**。
4. 在**云平台配置检查**面板，查看云平台配置检查项结果及其详情。



- **查看最近一次检查结果的统计**

  您可在云平台配置检查项列表上方，查看到有风险的检查项数量（**风险项**包括总数量和不同等级风险的检查项数量）、有风险的资产数量（**风险数**）、未启用检查项数量、已启用检查项数量统计及最近一次检查时间。

- **查看检查项**

  您可查看到云平台配置检查项列表信息，包括检查结果风险等级、影响资产类型及数量、检查项类型和最新检查时间等。

- **查看检查结果详情**

单击**基线检查项**名称，跳转到检查项的详情页面，查看对应的检查详情描述、可能产生的影响和处理建议。



处理云平台配置检查结果

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**云产品检查**。
4. 在**云平台配置检查**页面，处理云平台配置检查结果。
   - **验证**

     如果您对部分配置项进行了修改，在云平台配置检查项列表，定位到该配置检查项，单击操作栏的**验证**，检验新的配置是否存在安全风险。



   - **加白名单**

     如果您判断检测出的某个风险项不存在安全风险，可在云平台配置检查项列表，定位到该配置检查项，单击**加白名单**将该检查项状态调整为**已忽略**。**已忽略**的检查项将不会包含在**风险项**总数中。

在检查项列表中，您也可对**已忽略**的检查项**取消加白**。



> **说明** **加白名单**只对本次检测结果进行忽略，后续如果再次检测该出该风险，云盾安全中心仍会展示该检测结果的告警。

4.6. 资产中心

4.6.1. 查看服务器安全状态

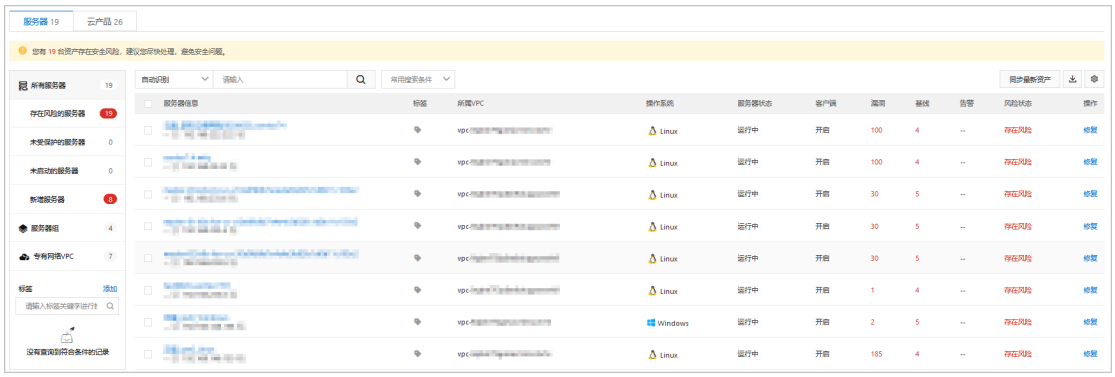
资产中心页面提供了所有服务器的安全状态相关信息，例如服务器的所属VPC、服务器状态、风险状态等统计信息。本文介绍如何通过筛选功能查看指定服务器的安全状态，并对搜索条件和显示信息进行设置。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**服务器**页签，查看服务器安全状态。

   您可以根据需要执行以下操作：

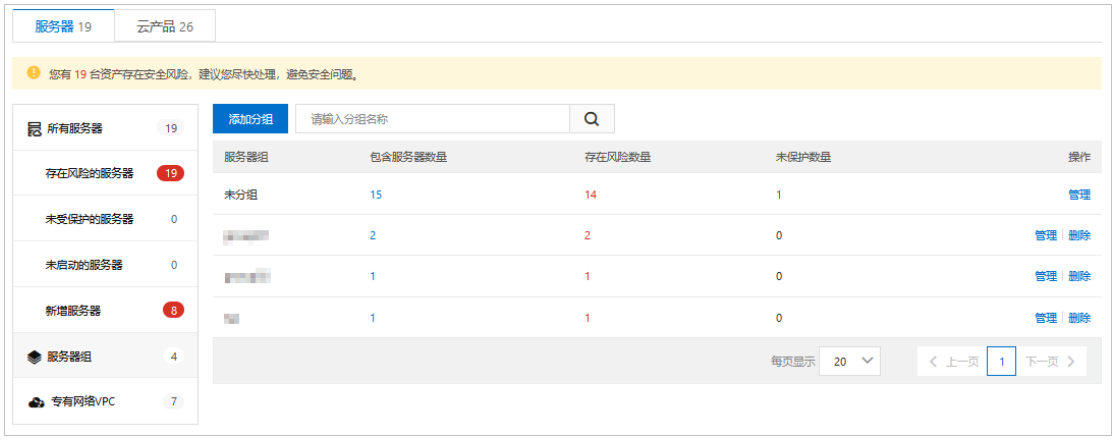
   - **根据服务器状态进行筛选**
     - 在**所有服务器**功能项，您可以查看**所有服务器**数量、**存在风险的服务器**数量、**未受保护的服务器**数量、**关机的服务器**数量和**新增服务器**数量，查看所有服务器安全状态。



单击需要查看服务器的名称或其**操作**栏的**修复**，可查看或修复该服务器的详细信息。更多详细内容请参见查看单个资产详情。

- 单击**存在风险的服务器**、**未受保护的服务器**、**关机的服务器**或**新增服务器**，查看对应服务器的安全状态。

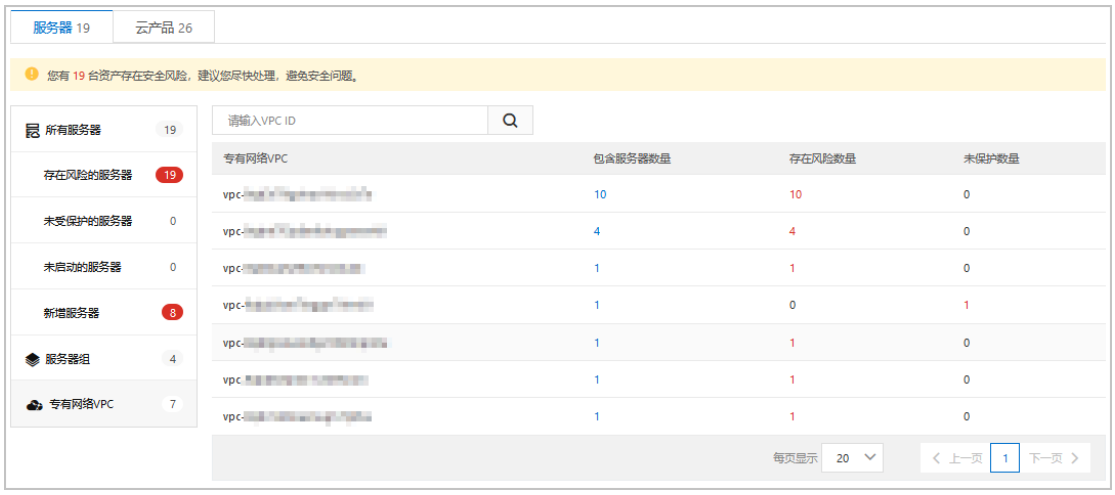
- **根据服务器组进行筛选**
  - 单击**服务器组**，您可以查看**服务器组**数量及各分组的**包含服务器数量**、服务器**存在风险数量**和**未保护数量**。



云盾态势感知支持**管理**和**删除**服务器分组，具体操作指导请参见管理资产分组。

  - 单击目标分组下**包含服务器数量**、**存在风险数量**或**未保护数量**，查看目标分组下服务器安全状态。

- **根据专有网络VPC实例ID进行筛选**
  - 单击**专有网络VPC**，您可以查看**专有网络VPC**数量及各VPC下的**包含服务器数量**、服务器**存在风险数量**和**未保护数量**。



  - 单击目标专有网络VPC下**包含服务器数量**、**存在风险数量**或**未保护数量**，查看目标VPC下服务器安全状态。

- **根据标签项进行筛选**

  您可以单击资产列表左侧已添加的标签项，查看对应标签下服务器的安全状态。

- **多筛选查看**

  使用**所有服务器**、**服务器组**、**专有网络VPC**或**标签**功能选项，通过**资产中心**列表上方搜索栏，筛选出指定的服务器。

- 展示多个筛选子项结果：

  您可以在**资产中心**列表上方搜索栏，选择识别类型（**公网IP**、**私网IP**、**实例名称**、**操作系统**、**是否有基线问题**、**是否有漏洞问题**、**是否有安全告警**、**是否存在风险**、**是否在线**、**标签名称**、**分组名称**、**操作系统类型**、**是否有快照风险**），并选择或输入指定类型信息，筛选出指定的服务器。

  > **说明**
  >
  > 您可以同时输入多个检索项，并选择多个检索项之间的关系。以下是检索项关系的相关说明：
  >
  > - 检索项之间的关系：
  >   - AND：检索项之间是**与关系**。
  >   - OR：检索项之间是**或关系**。
  > - 展示多个筛选子项结果，需要选择检索项之间的关系为OR。
  > - 需要输入指定信息搜索的检索项，完成输入后，需要单击**搜索**按钮，才能显示对应的检查信息。

- 展示跨筛选项组合结果：

  同时应用多个筛选项。

  您可以在选择了**服务器组**、**专有网络VPC**或**标签**功能检查后，通过**资产中心**列表上方搜索栏，筛选出更多指定的服务器。

- **设置常用筛选条件**

  对于已应用的筛选项组合，您可以将其保存为常用筛选条件。单击**保存**，在**保存条件**对话框为该筛选条件命名后，就可以在搜索栏右侧**常用搜索条件**选择框中直接选用该筛选条件。

- **设置显示列**

  单击**资产中心**页面右上角的 图标，可以设置需要显示的列内容。

4.6.2. 查看云产品安全状态

资产中心页面提供了云产品安全状态的相关信息，包括存在风险云产品信息及云产品分类（负载均衡、NAT网关）统计等。本文介绍如何通过筛选功能定位查看目标云产品安全状态，并对搜索条件进行设置。

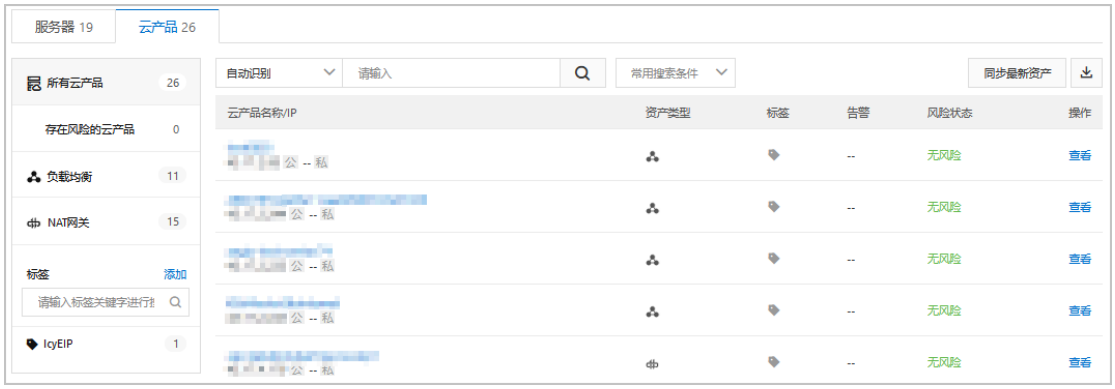
操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**云产品**页签，查看云产品安全状态。

   您可以根据需要执行以下操作：

   - **根据资产状态筛选云产品**

- 在**所有云产品**区域，您可以查看**所有云产品**数量和**存在风险的云产品**数量，查看所有云产品安全状态。



- 您可以单击**存在风险的云产品**，查看对应云产品的安全状态。

单击需要查看的云产品名称或其操作列的**查看**，可查看目标云产品的详细信息。更多详细信息请参见查看单个资产详情。

- **根据资产类型进行筛选**

云产品资产类型分为以下2种：

- **负载均衡**
- **NAT网关**

在各资产类型功能项，您可以查看对应资产类型的云产品数量。单击**负载均衡**、**NAT网关**，查看对应云产品的安全状态。

- **根据标签项进行筛选**

您可以在**标签**功能项中，查看标签对应资产数量。单击资产列表左侧已添加的标签项，查看对应标签下云产品的安全状态。

- **多筛选查看**

使用**所有云产品**、**负载均衡**、**NAT网关**功能选项，通过**资产中心**列表上方搜索栏，筛选出指定的资产。

例如，选择**所有云产品**，进行多筛选查看资产安全状态。

- 展示多个筛选子项结果：

  您可以在**资产中心**列表上方搜索栏，选择识别类型（**公网IP**、**实例名称**、**是否有安全告警**、**是否存在风险**、**标签名称**、**分组名称**），并选择或输入指定类型信息，筛选出指定的资产。

  > **说明**

- 展示跨筛选项组合结果：

  同时应用多个筛选项。

  - 您可以在选择**负载均衡**、**NAT网关**或**标签**功能检查后，通过**资产中心**列表上方搜索栏，筛选出更多指定的资产。
  - 您也可以在选择**所有云产品**、**负载均衡**、**NAT网关**功能检查后，通过**标签**项，筛选出更多指定的资产。

- **设置常用筛选条件**

对于已应用的筛选项组合，您可以将其保存为常用筛选条件。单击**保存**，在**保存条件**对话框为该筛选条件命名后，就可以在搜索栏右侧条件框中直接选择该筛选条件。

4.6.3. 查看单个资产详情

资产中心功能提供了所有资产的详细信息，包括基本信息、漏洞信息、安全告警处理、基线检查和资产指纹调查等。本文介绍了查看单个服务器或云产品的信息的具体操作。

背景信息

资产中心页面，提供了所有资产的基本信息。根据资产类型不同，对服务器和云产品提供的管理功能是不同的。

下表罗列云盾安全中心的**资产中心**页面提供的服务器与云产品详情的功能差异，其中用到的标识：

- X：表示不包含在服务范围中。
- √：表示包含在服务范围中。

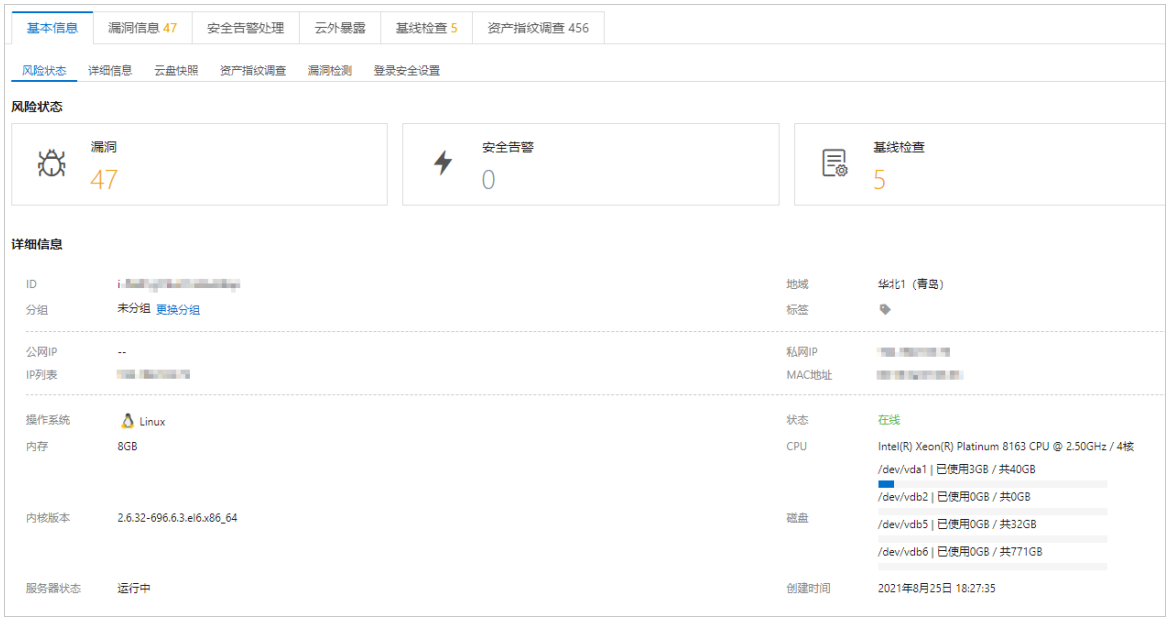
功能项	功能项内容	服务器	云产品
基本信息	风险状态：展示该资产风险的数量统计，包括以下类型： • **漏洞** • **安全告警** • **基线检查**	√	√（仅支持安全告警处理功能）
	详细信息：展示该资产的配置和保护状态等信息，支持配置该资产的分组和标签。	√	√（不支持资产分组功能）
	资产指纹调查：展示该资产指纹（端口、软件、进程、账户）的统计信息。	√	X
	漏洞检测：展示漏洞检测类型，支持为该资产开启或关闭不同类型的漏洞检测功能。	√	X
	登录安全设置：展示该资产已添加的常用登录地址、登录的IP、时间和账号，支持设置该资产的相关告警。	√	X
漏洞信息	展示该资产的漏洞检测结果。	√	X
安全告警处理	展示该资产的安全告警信息。	√	√
基线检查	展示该资产的基线检查结果。	√	X
资产指纹调查	展示该资产指纹的详细信息。	√	X

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**资产中心**页面单击**服务器**或**云产品**页签。

5. 在**服务器**或**云产品**页面，定位到目标资产并单击其名称。
6. 查看单个资产详情。

   在当前资产详情页面，单击**基本信息**、**漏洞信息**、**安全告警处理**、**云外暴露**、**基线检查**或**资产指纹调查**页签查看资产信息。



以下介绍了该资产的相关信息：

- **基本信息**：选择各功能页签查看和管理资产相关信息。
  - **风险状态**：查看漏洞、安全告警、基线检查的检测结果统计信息。单击对应统计数值可跳转至对应页面查看详细信息。

- **详细信息**：查看资产配置和保护状态等信息，并管理资产标签和分组。
  - **更换分组**

    单击**更换分组**，在**更换分组**对话框，选择新的分组，并单击**确定**。

  - **设置标签**

    单击图标，在**添加标签**对话框，选择标签并单击**确定**。

    单击已有标签右侧的图标，可删除资产所属标签。

- **资产指纹调查**：查看资产指纹的统计信息。单击对应统计数值可跳转至**资产指纹调查**页签查看指纹详细信息。



- **漏洞检测**：查看该资产已开启或关闭的漏洞检测功能项，您可根据需要为该资产开启或关闭不同类型的漏洞检测功能，覆盖的漏洞类型包括：Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞和应急漏洞。
- **登录安全设置**：设置**常用登录地**和高级登录（IP、时间、账号）报警功能；**开启或关闭**非合法登录（IP、时间、账号）报警功能；为目标资产添加常用登录的IP、时间和账号。



- **漏洞信息**：查看目标资产下漏洞检测结果。



- **安全告警处理**：查看目标资产下安全告警检测结果。
- **基线检查**：查看目标资产下基线检查结果。



- **资产指纹调查**：查看并采集目标资产下指纹（端口、进程、软件、账户）调查统计信息。

  您可手动触发资产指纹数据的采集，获取目标资产指纹的最新数据。

  a. 选择**端口**、**软件**、**进程**、**账户**、**计划任务**页签，并单击页面右上方**立即采集数据**。

b. 在**采集数据任务下发成功**对话框中，单击**确定**。



采集数据任务下发成功后，需要1~5分钟才能完成指纹数据的采集。任务结束后，您可查看到目标资产的最新指纹数据。

4.6.4. 开启和关闭服务器保护状态

本文介绍如何开启和关闭资产的保护状态。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**服务器**页签中，为指定服务器开启或关闭保护。
   - **开启保护**

     选中一个或多个客户端实时防护状态为**关闭**的目标服务器，并选择**更多操作 > 开启保护**。

     防护状态开启后，目标服务器的客户端实时防护状态变为**开启**。
   - **关闭保护**

     如果您确认服务器无需云盾安全中心的防护，可以为服务器关闭保护。选中一个或多个**客户端**实时防护状态为**开启**的目标服务器，并选择**更多操作 > 暂停保护**。

     > **说明** 服务器关闭防护后，云盾安全中心将无法再为服务器提供安全防护，包括漏洞检测、安全告警等。建议您谨慎操作。

     关闭成功，目标服务器的**客户端**实时防护状态变为**关闭**。

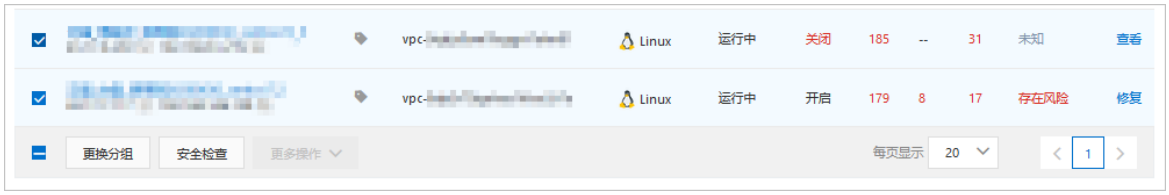
4.6.5. 一键安全检查

资产中心页面的服务器页面提供了安全检查功能，支持对指定服务器下发安全扫描任务，包括漏洞检测、基线检测、网站后门检测、资产指纹（端口、软件、进程、账号）采集。本文介绍了服务器安全检查功能的具体操作。

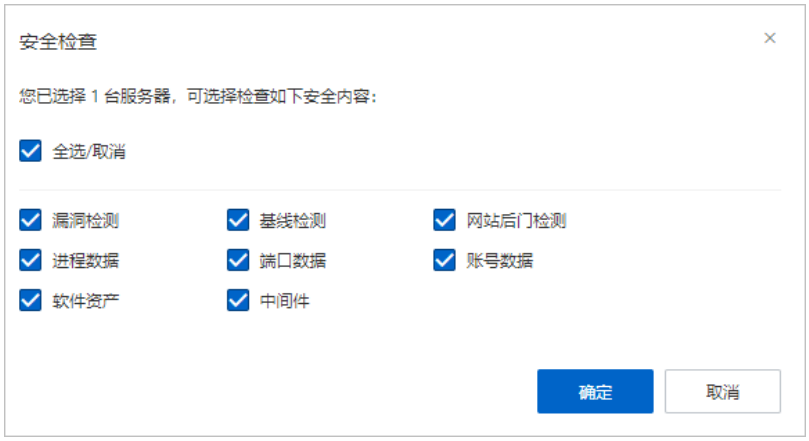
操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**服务器**页签的列表中，选中一个或多个需要执行安全检查的服务器。

5. 单击列表下方的**安全检查**。



6. 在**安全检查**对话框中，选中需要执行的检查项目。



7. 单击**确定**，执行检查。
8. 在提示对话框中，单击**确定**。



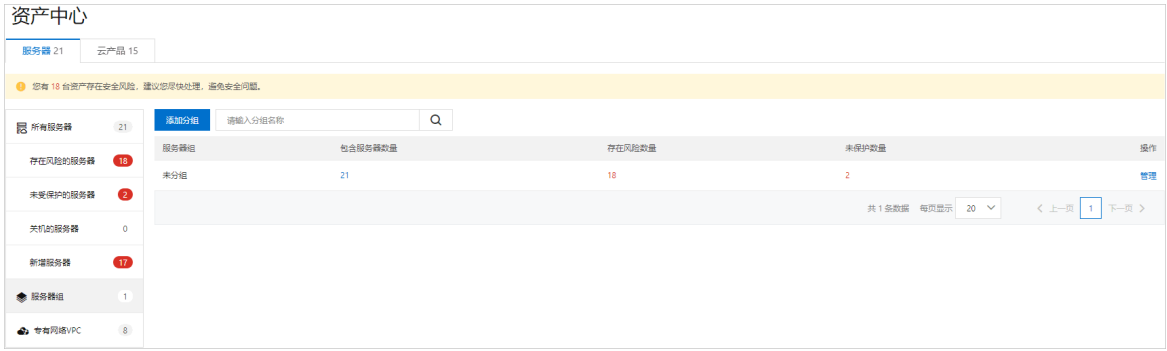
一键安全检查结束后，最新的检查结果会自动更新到云盾控制台态势感知资产中心该资产的详情页面。

4.6.6. 管理资产分组

本文介绍了服务器分组功能的添加、修改、删除、更换的具体操作。

添加分组

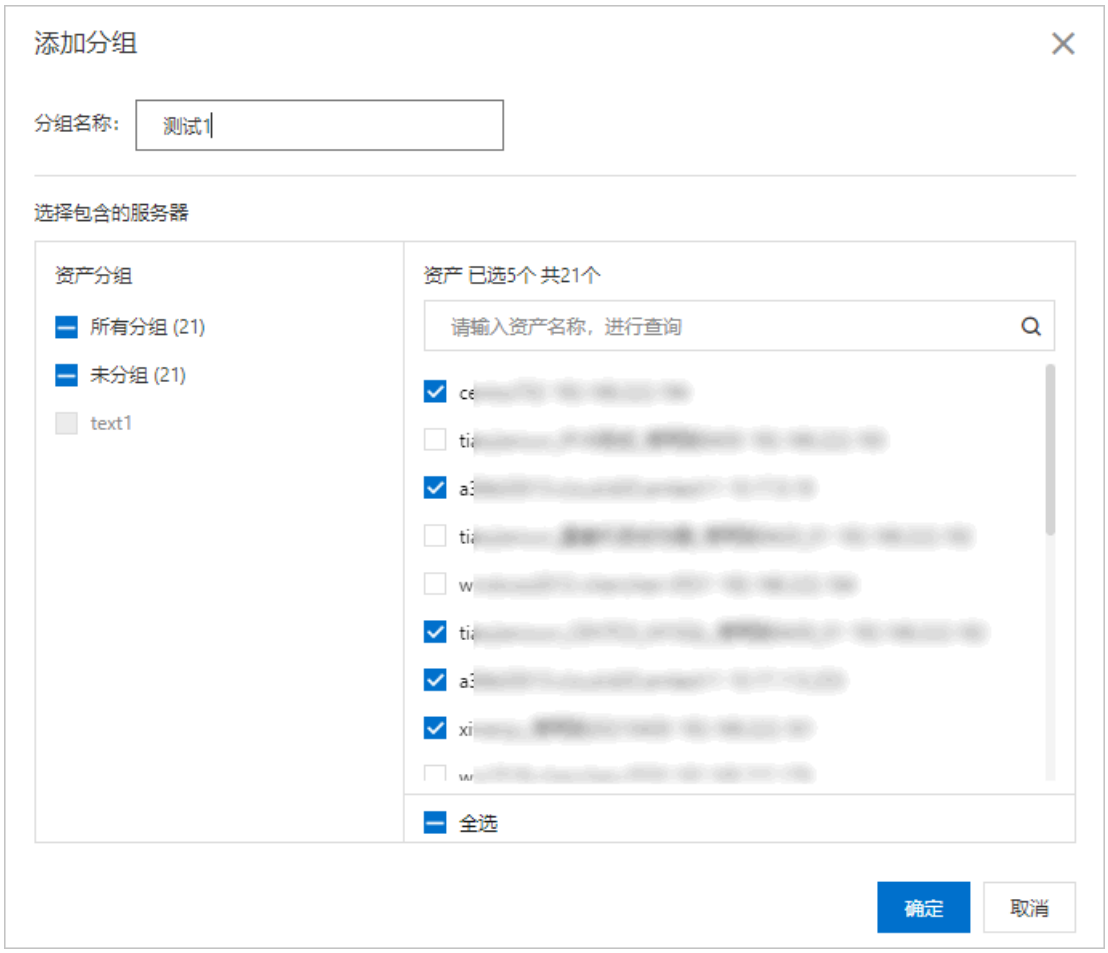
1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**服务器**页签列表左侧，单击**服务器组**。



说明 未进行资产分组时，所有的资产默认在**未分组**中。

5. 单击**添加分组**。
6. 在**添加分组**对话框，完成新分组的设置。

   您可以参考以下子步骤配置分组的参数。



   i. 在**分组名称**文本框输入分组名称。

   ii. 添加资产到新创建的分组。

   将未分组或已分组下的资产添加或转移至新创建的分组中。在**资产分组**中单击**未分组**或其他分组，在右侧**资产**列表选中资产。

7. 单击**确定**。

在服务器分组列表，您可以看到新创建的分组记录。

修改和删除分组

如果需要对某个分组进行修改（例如，修改分组名称或分组下的服务器）或删除，可参见以下步骤：

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**服务器**页签列表左侧，单击**服务器组**。
5. 定位到需要修改或删除的分组，单击**管理**或**删除**。

   您可以根据需要进行以下操作。

   - **修改分组**
     a. 单击需要修改分组操作列下的**管理**，打开分组管理对话框。
     b. 在**分组管理**对话框中的**资产分组**区块下，单击您要修改的分组。
     c. 在右侧的**资产**列表中，将您要修改的资产取消选中。
     d. 单击**确定**，完成资产分组的修改。
   - **删除分组**

     您可以单击一个分组右侧操作列下的**删除**，然后单击**确定**，即完成分组的删除。

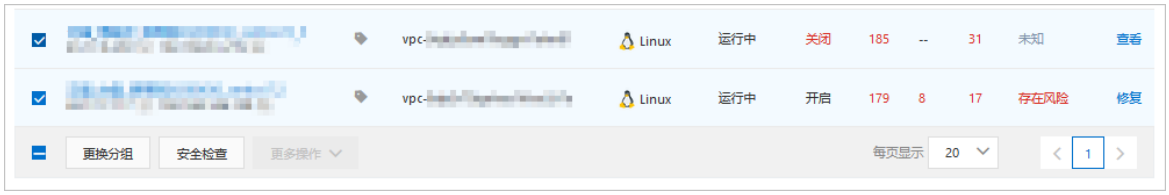
     > **说明** 当您删除某个分组时，该分组中的资产默认被移入**未分组**中。

更换服务器分组

您可以将多个同类型资产添加到一个分组中，便于对这些资产执行批量操作。如在配置基线检查策略模板时，按组别配置生效服务器；在资产列表页面，使用组别筛选并查看特定资产。

参照以下步骤，将资产添加到指定服务器分组中：

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在服务器列表页，选中一个或多个服务器资产并单击资产列表下方的**更换分组**。



5. 在**更换分组**对话框，选择新的服务器分组。



6. 单击**确定**。

4.6.7. 管理资产标签

本文介绍了服务器资产重要性标签的添加和自定义标签的添加、修改和删除的具体操作。

背景信息

云盾安全中心提供以下表格中的资产重要性标签，方便您根据重要性快速对资产进行分类。您可以为您的资产选择相应的重要性标签。

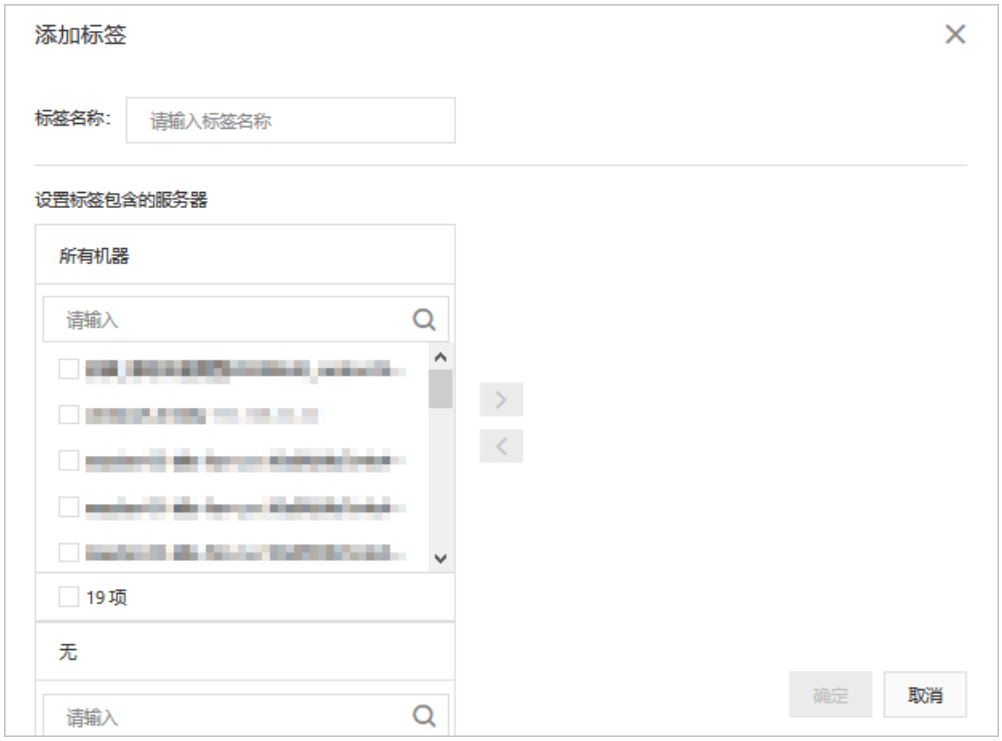
您为资产设置的重要性标签决定了漏洞修复紧急度得分计算方法中的**资产重要性因子**。**资产重要性因子**会影响资产的漏洞修复紧急度得分。根据漏洞修复紧急度得分您可以判断一个漏洞是否被优先修复。建议您为核心资产设置重要性标签，云盾安全中心将根据资产重要性提示您尽快修复重要资产中的漏洞。以下表格展示了资产重要性标签和资产重要性因子取值的关系。

重要性标签类型	资产重要性因子	选择建议
重要资产	1.5	运行您核心业务或存储核心数据的资产，该类资产被病毒恶意入侵会对业务系统造成较大影响并导致重大的业务损失。
一般资产	1	运行一般业务的资产，可替代性较高。该类资产被病毒恶意入侵后对整个系统的影响较小。
测试资产	0.5	进行业务功能或性能测试的资产，或其他对您业务影响较小的资产。

说明 如果您未设置资产重要性标签，您所有资产的重要性标签默认为**一般资产**，即所有资产重要性因子都为1。

添加自定义标签

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**资产中心**页面，单击**服务器**或**云产品**页签。
5. 在**服务器**或**云产品**页面，单击资产列表左侧筛选功能**标签**右侧的**管理**。
6. 在**添加标签**对话框中的**标签名称**文本框中输入标签名称。



7. 在左侧**资产分组**区域框中，单击分组名称，在右侧**资产**列表中，选中您要添加的资产添加至新创建的标签。
8. 单击**确定**。

   您可以在资产列表，单击目标资产**标签**栏的 图标，将该资产添加至已创建的标签。

> **说明** 一个资产支持添加多个标签，每个资产的所属标签都会在资产列表的**标签**栏显示。

修改和删除自定义标签

如果需要对某个标签进行修改（例如：修改标签名称或修改标签添加的服务器）或删除，可参见以下步骤：

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**资产中心**。
4. 在**资产中心**页面，单击**服务器**或**云产品**页签。
5. 在**服务器**或**云产品**页面，修改或删除标签。

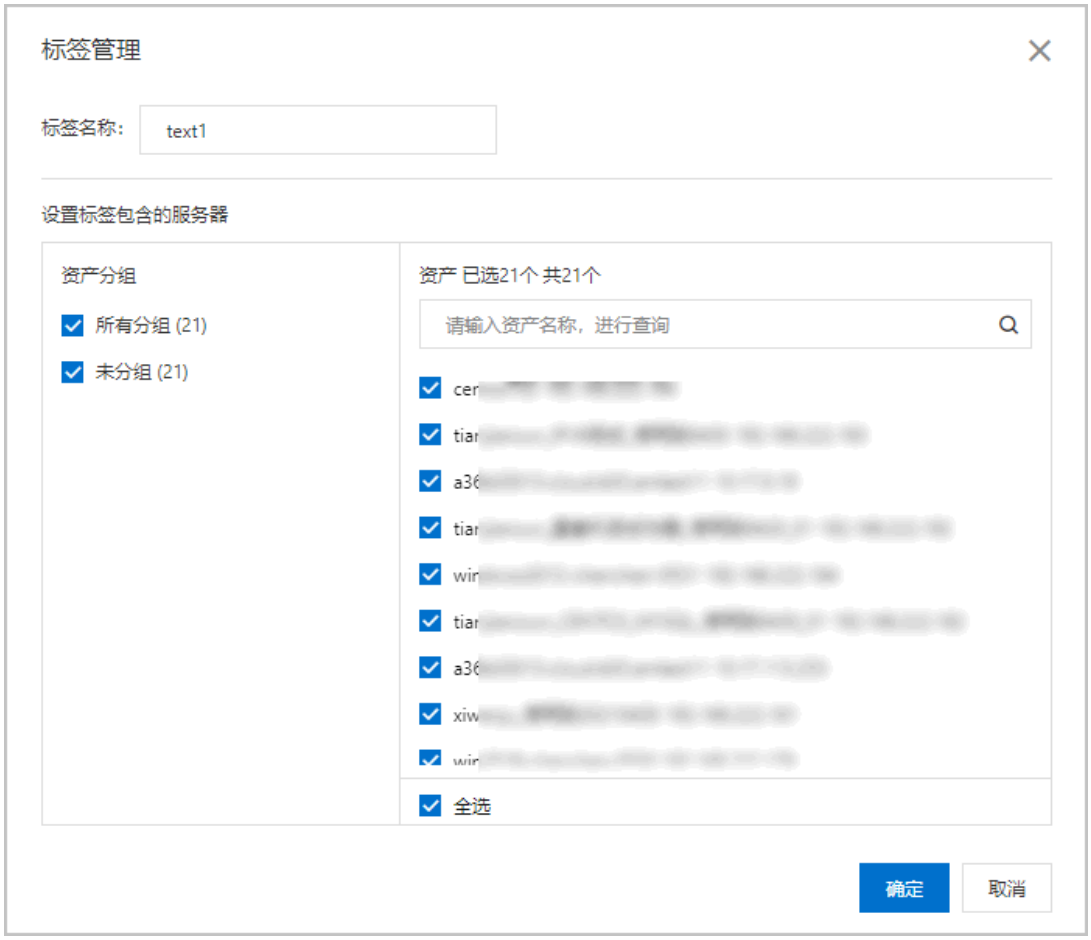
   您可以参考以下步骤修改或删除标签：

   - **修改标签**

a. 如果需要修改单个标签，可将鼠标悬浮在该标签栏中，单击显示的 图标。



b. 在**标签管理**对话框中修改**标签名称**，或添加、删除标签下的服务器。



c. 单击**确定**。

- **删除标签**

  如果需要删除某个标签，可将鼠标移动至该标签栏中，单击显示的 图标，并单击**确定**，删除标签。



4.7. 应用白名单

应用白名单可防止服务器上有未经过认证或授权的程序运行，提供可信的资产运行环境。

背景信息

应用白名单功能支持将需要重点防御的服务器加入到白名单中，通过检测白名单中指定的应用程序区分可信、可疑和恶意程序，防止未经白名单授权的程序运行。可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。

在创建白名单策略之后，您可以通过在需要重点防御的服务器中应用该白名单策略，云盾安全中心将检测服务器中是否存在可疑或恶意进程，并对不在白名单中的进程进行告警提示。

> **说明** 不在白名单中的程序启动时会触发安全告警。云盾安全中心检测到的非白名单程序启动，可能是新启动的正常程序，或是被入侵后植入的恶意程序。如果提示告警的应用为正常程序、常用程序或者您安装的第三方程序，建议您将该程序加入白名单。已加入白名单的程序再次启动时将不再触发告警；如果该进程为恶意程序，建议您及时清理该进程，并查看计划任务等配置文件是否被篡改。

步骤一：配置应用白名单策略

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**应用白名单**。
4. 在**应用白名单**页面，单击**策略管理**页签。
5. 在**策略管理**页面，单击**创建策略**。
6. 在**创建白名单策略**页面完成以下配置：
   - **策略名称**：自定义白名单策略的名称。
   - **智能学习时长**：选择策略的智能学习时长，可选1天、3天、7天或15天。智能学习功能通过机器学习引擎实现自动化聚类和搜集大量告警数据，帮助提升对可疑或恶意进程的识别能力。
   - **智能学习服务器**：选中需要加入到该白名单的服务器。
7. 单击**下一步**，完成白名单策略的创建。
   白名单策略创建完成后，该策略的详情将会自动展示在策略列表中。



以下表格介绍白名单策略列表的参数。

参数	描述
策略名称	创建的白名单策略的名称。
生效服务器	应用该白名单策略的服务器数量。
状态	策略的生效状态。包含以下状态： ○ **策略已生效**：该策略已完成智能学习，并且已应用到服务器中。 ○ **智能学习完成，待确认**：该策略已完成智能学习，需确认并启用策略。 智能学习完成后，您还需单击该策略**策略状态**下的开启按钮启用该策略。启用策略后，策略才能生效，云盾安全中心会自动识别您服务器中进程的风险类型（可信、可疑和恶意）。 ○ **暂停**：智能学习被手动暂停。您可单击**继续**恢复智能学习功能。 ○ **学习中**：智能学习进行中。 策略创建完成后，云盾安全中心会对其自动执行智能学习。新创建的策略状态都为**学习中**。
应用	表示应用该策略的服务器中各类进程的分布情况，包含**可信**、**可疑**和**恶意**类型进程的数量。
操作	可对该策略执行的操作。支持进行以下操作： ○ **应用**：单击**应用**打开**应用白名单策略**面板，可增加或删除应用该策略白名单的服务器。 ○ **编辑**：单击**编辑**打开**编辑策略白名单**面板，对该策略进行修改。可修改该策略的**策略名称**、**智能学习时长**和需自动执行智能学习的服务器。 ○ **暂停学习**：暂停智能学习。 ○ **继续**：继续执行智能学习。 单击**继续**，该策略的状态会转为**学习中**，您可在**状态**栏查看策略的学习进度。 ○ **删除**：删除策略。 策略删除后，对应的服务器进程将不再受到该策略的保护。

步骤二：将服务器添加到应用白名单

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**应用白名单**。
4. 在**应用白名单**页面，单击**生效服务器**
5. 在**生效服务器**页签，单击**添加服务器**。
6. 在**添加服务器**页面,完成相应配置。

   在**添加服务器**页面您可以参考以下内容完成参数配置：

   ○ **白名单策略**：从策略列表中选择已创建的白名单策略。

   ○ **异常处理模式**：默认为**告警**，表示云盾安全中心检测到了可疑进程。

不在白名单内的服务器进程启动时，会自动触发告警。您可单击**异常行为数**一栏的告警数量，跳转到该服务器**资产中心 > 安全告警处理**页面，查看这些告警的详细信息。

- **生效服务器**：选中需要添加到该白名单的服务器。支持选择多台服务器。

  您可通过在**生效服务器**搜索框输入服务器名称，搜索需要添加到白名单的服务器。**生效服务器**名称支持模糊查询。

7. 单击**确认**完成服务器的添加。
   应用白名单创建完成后，您可以在**生效服务器**页面的服务器列表中，查看您已添加到应用白名单的服务器和该服务器使用的白名单策略名称。

   生效服务器页面展示应用了白名单策略的服务器的以下信息：

   - **服务器/IP**：应用了白名单策略的服务器名称和IP地址。
   - **白名单策略**：该服务器应用的白名单。
   - **异常行为数**：不在白名单策略中，并且已启动的进程数量。异常进程启动时，会触发云盾安全中心的检测机制，并进行实时告警。
   - **异常处理模式**：默认为**告警**，表示云盾安全中心检测到了可疑进程。

     不在白名单内的服务器进程启动时，会自动触发告警。您可单击**异常行为数**一栏的告警数量，跳转到该服务器**资产中心 > 安全告警处理**页面，查看这些告警的详细信息。
   - **操作**：单击**操作**栏的**删除**会将该服务器从应用白名单中删除。

     删除后，白名单策略会对该服务器失效，服务器进程启动时云盾安全中心将会对其进行告警提示。

将进程加入或取消白名单

服务器配置了应用白名单后，您可以在**生效服务器**页面的服务器列表中，查看您已添加到应用白名单的服务器和该服务器使用的白名单策略名称。您可在**白名单策略**栏中单击对应的策略名称，打开该服务器的白名单进程列表，查看服务器中检测到的可信、可疑和恶意进程及其详细信息。

白名单策略列表中包含服务器进程的以下信息：

- **类型**：该白名单服务器中运行的进程类型，分为可信、可疑和恶意3种类型。
- **进程名称**：该白名单服务器中的进程。
- **Hash**：进程的哈希函数。哈希函数用于判断进程的唯一性，避免程序被恶意伪造。
- **路径**：进程在服务器中的文件路径。
- **可信程度**：云盾安全中心判断该进程的可信任程度，分为0%（恶意进程）、60%（可疑进程）、100%（可信进程）。

  > **说明** 建议您对可信程度为0%的恶意进程进行重点排查和处理。

- **操作**：对该进程可执行的操作。您可结合服务器上业务的部署情况确定是否要将该进程加入白名单。 您可以进行以下操作：
  - **加入白名单**：将进程加入白名单表示信任该进程。
  - **取消白名单**：将进程从白名单中取消表示云盾安全中心将该进程标识为不可信进程，该进程启动后将触发告警。

4.8. 漏洞扫描

4.8.1. 快速入门

本文介绍如何快速使用漏洞扫描功能。

漏洞扫描的使用流程如下：

1. 根据自身实际环境需要，配置漏洞扫描的检测项目和检测周期。
   - 配置全局监控：包括开启的检测功能和各功能的检测周期，请参见配置全局监控。
   - 配置基础监控：包括弱口令漏洞、运维安全漏洞、CMS应用漏洞和基线监控等，请参见配置基础监控。
   - 配置Web监控：包括检测周期、监控的Web漏洞类型，请参见配置Web监控。
   - 配置白名单：把不需要检查的资产放入白名单中，请参见配置白名单。
2. 导入需要进行漏洞扫描检测的资产。
   - 导入私有资产：通过配置扫描引擎导入VPC下的私有资产，请参见配置扫描引擎（私有资产）。
   - 导入公网资产：通过导入资产方式导入，请参见导入资产。

   > **说明** 导入的资产数量需要少于或等于许可的最大资产数量。

3. 查看和确认漏洞扫描结果。
   - 查看概览：查看整体的漏洞扫描结果，请参见查看概览。
   - 查看和确认安全漏洞风险：请参见管理安全漏洞风险。
   - 查看和确认主机合规风险：请参见管理主机合规风险。
   - 查看和确认外部风险：即查看外部代码泄漏的风险，请参见管理外部风险。
4. 输出漏洞扫描报表。

   通过报表方式周期性审查资产的漏洞和基线安全，请参见创建报表。

4.8.2. 查看概览

本文介绍漏洞扫描的整体结果，以便安全管理员快速了解和掌握当前的漏洞情况。

背景信息

漏洞扫描功能识别的漏洞包括：Web安全漏洞、CMS应用漏洞、弱口令漏洞、运维安全漏洞和基线安全漏洞。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**概览**。
4. 查看漏洞扫描的整体结果。



区域	说明
今日关注	查看今日的资产概览、未修复风险和已修复风险。 ○ **资产概览**：显示今日的主机数、网站数和域名数，并对当前的资产进行安全评分。 右侧的雷达图展示Web安全漏洞、CMS应用漏洞、弱口令漏洞、运维安全漏洞和基线安全漏洞的分布状况。 ○ **未修复风险**：显示今日的高危、中危、低危和总的未修复风险数量。 右侧的**未修复风险分布**展示未修复风险的分布状况。 ○ **已修复风险**：显示今日的高危、中危、低危和总的已修复风险数量。 右侧的**已修复风险分布**展示已修复风险的分布状况。
资产风险TOP5	通过按钮选择，分别查看**安全漏洞**和**主机合规**的Top5资产风险。 Top5的资产风险支持按照资产或者分组的形式展示。
风险监控趋势	通过按钮选择，分别查看**安全漏洞**和**主机合规**的风险变化趋势图。 图中以不同颜色的线条区分未修复风险和已修复风险，鼠标放在线条上可以查看当日未修复风险和已修复风险的数量。
资产监控趋势	查看受保护主机和网站的数量变化趋势。 图中以不同颜色的线条区分主机和网站，鼠标放在线条上可以查看当日受保护主机和网站的数量。
风险资产排行榜	通过按钮选择，分别以**按最新风险**和**按高危风险**的方式，查看风险资产排行。
端口服务统计	通过按钮选择，分别以**端口**和**主机服务**的维度统计情况。

4.8.3. 资产管理

4.8.3.1. 查看资产分析

本文介绍如何查看网站资产和主机资产的分析情况。

背景信息

通过资产分析，查看网站资产的网站服务、开源架构、设备类型和查看主机资产的主机端口、主机服务、操作系统等信息。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在**漏洞扫描**界面左侧导航栏中，单击**资产**。
4. 在**资产**界面，单击**资产分析**，查看网站资产。



5. 查看主机资产。



4.8.3.2. 导入资产

本文介绍如何导入公网资产。

背景信息

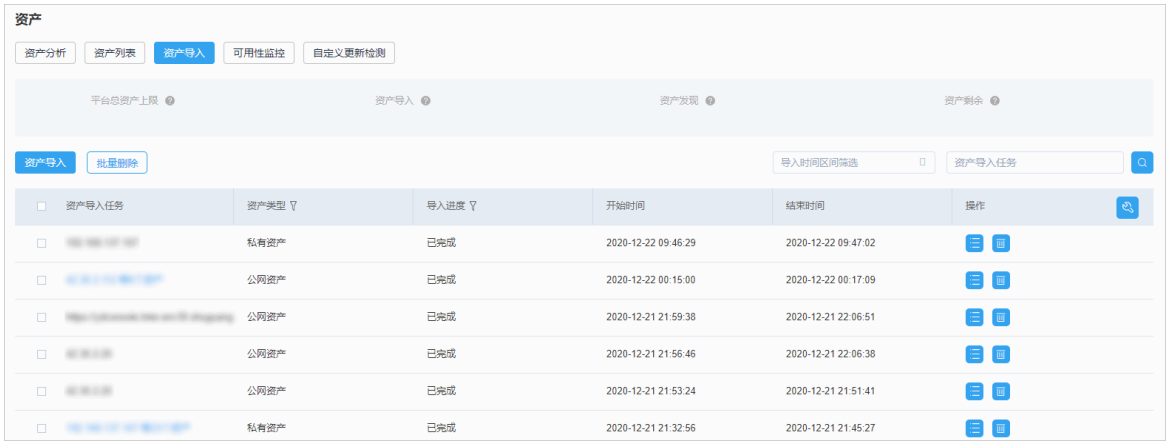
漏洞扫描功能只对已导入的资产进行漏洞扫描，所以在对资产进行漏洞扫描前，需要先导入资产。

漏洞扫描功能支持的资产包括公网资产和私有资产（VPC）。

- 私有资产的导入，需要添加扫描引擎，具体步骤，请参见配置扫描引擎（私有资产）。
- 公网资产的导入，可以参见本文。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在**漏洞扫描**界面左侧导航栏中，单击**资产**。
4. 在**资产**界面，单击**资产导入**页签，查看已导入资产。



5. 单击**资产导入**，进入**公网资产导入**界面，创建资产导入任务。
   i. 在**导入资产**区域，选择**手工导入**方式，在输入框中输入资产，选中免责声明。
      - 资产支持域名、URL、IP、IP段等方式。
      - 支持批量导入，各资产间使用回车键分隔。
      - 资产不要包含有VPC的资产。
      - 导入资产数量需要少于平台总资产剩余数量。

> **说明** 例如平台总资产剩余数量为100个，如果此处输入的资产数量为90个，则输入的资产都能进行漏洞扫描；如果此处输入的资产数量为110个，则只能保护其中100 个资产，剩余10个资产不能进行漏洞扫描。

ii. 在**资产信息**区域，为导入的资产进行分组、设置负责人和设置资产标签。

- 在**资产分组**下拉菜单中选择分组，可以通过单击图标进行新增、编辑和删除分组。
- 在**负责人**下拉菜单中选择具体的资产负责人，可以通过单击图标进行新增、编辑和删除负责人。
- 在**资产标签**右侧，单击**添加标签**，为导入资产添加标签。

iii. 在**导入设置**区域，设置导入后资产操作。

功能		说明
资产发现	*自动导入子域名*	对于导入的域名，自动查询子域名资产。
	自动导入关联IP	自动添加域名解析的IP资产。
	自动同步标签及分组	系统发现的新资产与本次导入资产同步分组和标签。
网站资产	*开启WEB监控*	对于导入的网站资产，开启Web监控功能。 单击图标，可以选择使用的Web监控规则，具体如何设置Web监控规则，请参见配置Web监控。

iv. 在**白名单**区域，添加不需要进行检测的资产。

输入格式支持IP和URL，如果添加多个资产，使用回车键分隔。

v. 单击**保存**。

6. 管理资产导入任务。

资产任务创建成功后，在任务列表中可以查看到新增任务，并支持以下操作。

操作图标	说明
	查看资产导入任务详情、导入结果和导入过程。
	删除资产导入任务。

4.8.3.3. 管理资产列表

本文介绍如何查看和管理资产列表。

背景信息

通过资产列表，可以查看资产信息。在资产的用途和责任人变动时，安全管理员可以同时更换资产的分组、负责人等信息。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在漏洞扫描界面左侧导航栏，单击**资产**。
4. 在**资产**界面，单击**资产列表**页签，查看资产列表。



5. 单击**网站资产**页签，管理网站资产。
   i. 通过设置过滤条件，筛选网站资产。

      通过筛选功能，快速筛选出目标资产。

过滤条件	说明
资产类型	选择资产类型，例如公网资产、具体的VPC。
资产来源	选择资产来源，包括**手工导入**、**系统发现**。
资产分组	选择资产所属的分组。
网站状态	选择网站状态。
负责人	选择网站所属的负责人。
资产变动	选择资产的变动情况，包括**全部**、**新上线**、**有更新**、**无更新**、**已下线**。
网站监控	选择资产的网站监控状态。
风险等级	选择资产的风险等级。
网站服务	选择网站的服务类型及版本。
WAF识别	选择WAF的识别状态。
开源框架	选择资产的开源框架类型。
设备类型	选择设备类型。
资产导入时间范围	选择资产导入的时间范围。
资产关键信息	输入资产的关键信息，关键字包括网站、域名、IP、标题、标签。

   ii. 单击**一键导出**，将资产列表导出为Execl格式。

iii. 选中单个或者多个网站地址，管理网站资产。管理网站资产操作及说明，见下表：

操作	说明
批量WEB监控	批量开启和关闭Web监控。 ■ 批量开启Web监控：在下拉菜单中，单击**批量开启监控**。 ■ 批量关闭Web监控：在下拉菜单中，单击**批量停止监控**。
更换分组	批量更换资产的分组。
更换负责人	批量修改资产的负责人。
批量删除	批量删除资产，删除后资产将不受漏洞扫描功能的防护。

6. 单击**主机资产**页签，管理主机资产。

i. 通过设置过滤条件，筛选主机资产。

通过筛选功能，快速筛选出目标资产。

过滤条件	说明
资产类型	选择资产类型，例如公网资产、具体的VPC。
资产来源	选择资产来源，包括**手工导入**、**系统发现**。
资产分组	选择资产所属的分组。
负责人	选择资产所属的负责人。
资产变动	选择资产的变动情况，包括**全部**、**新上线**、**有更新**、**无更新**、**已下线**。
风险等级	选择资产的风险等级，包括**全部**、**高危**、**中危**、**低危**、**安全**。
存活状态	选择资产的存活状态，包括**存活**、**关闭**。
操作系统	选择主机的操作系统。
主机端口	选择主机的端口。
CDN识别	选择资产是否有CDN识别。
主机服务	选择主机资产的服务。
资产导入时间范围	选择资产导入的时间范围。
资产关键信息	输入资产的关键信息，关键字包括IP、主机、标签、关联域名。

ii. 单击**一键导出**，将资产列表导出为Execl格式。

iii. 选中单个或者多个主机地址，管理主机资产。管理主机资产的操作及说明，见下表：

操作	说明
更换分组	批量更换资产的分组。
更换负责人	批量修改资产的负责人。
批量删除	批量删除资产，删除后资产将不受漏洞扫描功能的防护。

4.8.3.4. 管理资产可用性

本文介绍如何管理资产的可用性。

背景信息

主机或网站在长期使用的过程中，可能因为故障导致不可用。通过可用性监控，安全管理员可以了解到资产的可用性情况。对于不可用资产，安全管理员可以及时进行检查和分析问题。

资产可用性监控使用HTTP监控和PING监控两种方式：

- HTTP监控用于监控网站资产。
- PING监控用于监控主机资产。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在**漏洞扫描**界面左侧导航栏，单击**资产**。
4. 在**资产**界面，单击**可用性监控**，查看资产可用性监控任务列表。



5. 新增资产可用性的监控任务。

   可用性监控任务支持HTTP监控和PING监控两种方式。

   - HTTP监控方式的创建步骤如下：

     a. 单击**添加监控**。

b. 单击**HTTP监控**页签。



c. 设置监控参数。

配置项	说明
监控名称	设置可用性监控任务名称。
监控目标	选择监控目标网站。
监控频率	选择监控网站间隔时间，可选**1 分钟**、**5 分钟**、**15 分钟**、**30 分钟**。
请求方法	监控网站时发送的HTTP请求包使用的请求方法，可选**HEAD**、**GET**、**POST**、**PUT**。
告警设置	设置监控异常告警，满足以下任一条件时，表示目标网站不可用。 ■ 响应时长，超过设置值表示异常。 ■ 响应状态，请求返回状态码异常。

d. 单击**保存**。

- PING监控方式的创建步骤如下：

a. 单击**添加监控**。

b. 单击**PING监控**页签。



c. 设置监控参数。

配置项	说明
监控名称	设置可用性监控任务名称。
监控目标	选择监控目标主机。
监控频率	选择监控主机间隔时间，可选**1 分钟**、**5 分钟**、**15 分钟**、**30 分钟**。
告警设置	设置监控异常告警，满足以下任一条件时，表示目标主机不可用。 ■ 响应时长，超过设置值表示异常。 ■ 响应状态，请求返回状态码异常。

d. 单击**保存**。

6. 批量管理监控任务。

   对于监控任务列表中的监控任务，可以批量进行管理。

   - 批量开启监控：

     选中多个监控任务，选择**批量监控管理 > 批量开启监控**。

   - 批量停止监控：

     选中多个监控任务，选择**批量监控管理 > 批量停止监控**。

   - 批量删除监控：

     选中多个监控任务，选择**批量监控管理 > 批量删除监控**。

4.8.3.5. 管理自定义更新检测

本文介绍如何管理自定义更新检测。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**资产**。
4. 在**资产**界面，单击**自定义更新检测**页签，查看自定义更新检测任务列表。
5. 新增自定义更新检测任务。
   i. 单击**添加检测**。
   ii. 在**添加自定义更新检测**页面，设置检测任务参数。



参数	说明
检测名称	设置自定义更新检测任务的名称。
检测目标	设置检测的目标资产，仅支持**公网资产**。 a. 根据需要，选择**主机资产**或者**网站资产**。 b. 在资产列表中，选中目标资产。 **说明** 可以通过**分组筛选**和**IP**快速搜索目标资产。

参数	说明
端口范围	检测的端口范围，支持**自定义**、**全端口**、**TOP100** 和**TOP1000**。 **说明** 只有**检测目标**为主机资产时，可以设置**端口范围**。 ■ **自定义**：自定义编辑需要扫描的端口。 ■ **全端口**：扫描所有端口。 ■ **TOP100**：扫描Top 100的端口。 ■ **TOP1000**：扫描Top 1000的端口。

iii. 单击**保存**。

4.8.4. 风险管理

4.8.4.1. 管理安全漏洞风险

本文介绍如何查看和处理漏洞扫描检测出来的安全漏洞风险。

背景信息

在**安全漏洞**页面，安全管理员可以查看通过漏洞扫描功能检测出来的安全漏洞。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**风险**。
4. 在**风险**界面，单击**安全漏洞**，查看安全漏洞风险。



   - 通过单击**未修复**或者**已修复**页签，可以切换查看**未修复风险**和**已修复风险**。
   - 查看风险统计信息，包括**未修复风险**、**已修复风险**、**未确认风险**、**已确认风险**、**已忽略风险**。
5. 通过选择**资产类型**、**风险等级**等信息搜索查询安全漏洞风险。
6. 处理安全漏洞风险。

   安全管理员根据风险列表中信息，分析和确认是否影响资产安全性。

   - 确认风险

     如果安全漏洞风险确认影响资产安全，在修复安全漏洞后，确认风险。

a. 单击目标风险**操作**列的图标。

b. 在下拉框中，单击**确认风险**。

c. 在提示框中，单击**保存**。

- 忽略风险

  如果安全漏洞风险存在误报（或者不影响资产安全），忽略风险。

  a. 单击目标风险**操作**列的图标。

  b. 在下拉框中，单击**忽略风险**。

  c. 在提示框中，单击**保存**。

7. 单击**一键导出**，导出安全漏洞风险列表到本地。

4.8.4.2. 管理主机合规风险

本文介绍如何查看和确认主机合规风险。

背景信息

在**主机合规**页面，安全管理员可以查看通过漏洞扫描功能检测出来的主机合规问题。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**风险**。
4. 在**风险**界面，单击**主机合规**页签，查看主机合规风险。

   通过单击**未修复**和**已修复**页签，可以切换查看**未修复风险**和**已修复风险**。



5. 通过选择**资产类型**、**风险等级**等信息搜索查询主机合规风险。
6. 处理主机合规风险。

   安全管理员根据风险列表中信息，分析和确认是否影响资产安全性。

   - 确认风险

     如果主机合规风险确认会影响资产安全，在加固主机后，确认风险。

     a. 单击目标风险**操作**列的图标。

     b. 在下拉框中，单击**确认风险**。

     c. 在提示框中，单击**确定**。

- 忽略风险

  如果主机合规风险存在误报（或者不影响资产安全），忽略风险。

  a. 单击目标风险**操作**列的图标。

  b. 在下拉框中，单击**忽略风险**。

  c. 在提示框中，单击**确定**。

7. 单击**一键导出**，导出主机合规风险列表到本地。

4.8.4.3. 管理外部风险

本文介绍如何查看和确认外部风险（代码泄漏）。

背景信息

在 **外部风险** 页面，安全管理员可以查看通过漏洞扫描功能检测GitHub仓库中的代码是否存在代码泄漏风险。

前提条件

已有GitHub账号并获取账号下的Token。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，选择 **风险 > 外部风险** 。
4. 单击 **代码泄漏** 页签。



5. 添加监控资产。

   i. 在 **资产监控列表** 区域，单击 **Token设置** 。

   ii. 在 **GitHub Token输入** 窗口，输入Token。

   支持批量输入，每个Token以回车键分隔。

iii. 单击 **添加资产** ，选择监控的外部资产。

6. 查看代码泄漏风险列表。

   通过单击 **未修复** 和 **已修复** 页签，可以切换查看未修复风险和已修复风险。

7. 处理代码泄漏风险。

   安全管理员根据风险列表中信息，分析和确认是否影响资产安全性。

   - 确认风险

     如果代码泄漏风险确认会影响资产安全，在加固主机后，确认风险。

   - 忽略风险

     如果代码泄漏风险存在误报（或者不影响资产安全），忽略风险。

4.8.4.4. 创建自定义风险检测

本文介绍如何创建自定义风险检测。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，选择**风险 > 自定义风险检测**。
4. 单击**添加检测**。
5. 在**添加自定义风险检测**页面，设置检测的参数。

参数	说明
检测名称	设置自定义风险检测名称。
检测目标	选择自定义的风险检测目标资产，支持**公网资产**。
应急检测	对于自定义风险检测，是否启用应急检测功能。 如果选择启用，则可以在列表中选择应急检测项。
基础风险检测	对于自定义风险检测，是否启用基础风险检测功能。 基础风险的监控配置请参见配置基础监控。
WEB风险检测	对于自定义风险检测，是否启用Web风险检测功能。 Web风险的监控配置请参见配置Web监控。

6. 单击**保存**。

4.8.5. 报表管理

4.8.5.1. 创建报表

本文介绍如何创建报表。

背景信息

通过创建报表，安全管理员可以查看一段时间内指定资产的安全风险情况，并执行应对的安全防护改进方案。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**报表**。
4. 在**风险报表**页面，单击**添加报表**。
5. 设置报表参数。



参数		说明
报表内容	**报表名称**	设置报表名称。
报表范围	**资产信息**	选择报表涉及的资产范围，支持**按单个资产**、**按资产分组**、**按全部资产**选项。 ○ **按单个资产**：选取单个的涉及资产。 ○ **按资产分组**：选取单个资产分组，同时支持选择标签。 **说明** 表示报表涉及的资产为该分组下拥有该标签的资产。 ○ **按全部资产**：支持按标签选择资产。
	发现时间	设置风险发现的时间范围。
	风险范围	选择报表的涉及的风险范围，支持选择**已修复风险**和**未修复风险**。

风险设置参数		说明
	风险类型	选择报表涉及的风险类型，支持选择**安全漏洞**和**主机合规**。

6. 单击**生成**。

执行结果

创建完报表后，**报表**页面的列表中会生成一条新的报表。

4.8.5.2. 批量删除报表

本文介绍如何批量删除报表。

背景信息

针对部分不再使用的报表，可以通过批量删除功能进行删除，节约存储空间。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**报表**。
4. 单击**风险报表**。
5. 在报表列表中，选中需要删除的报表。
6. 单击**批量删除**。

4.8.6. 配置管理

4.8.6.1. 配置全局监控

本文介绍如何对漏洞扫描进行全局监控配置，包括资产监控配置、基础风险监控配置、外部风险监控配置和扫描配置。

背景信息

通过设置全局监控，管理漏洞扫描中进行监控的项目、执行周期等信息。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**配置**。
4. 在**监控配置**页签下，单击**全局监控**。
5. 在**监控中状态**区域，查看全局监控状态。



6. 设置监控配置项。

   监控配置项包括**资产监控配置**、**基础风险监控配置**、**外部风险监控配置**和**扫描配置**。

   此处以设置**资产监控配置**为例，介绍配置步骤。



   i. 单击启用按钮，开启资产监控功能。

   - 启用按钮开启后，变为如上图所示蓝色的**已开启**状态；未开启时为灰色的**已关闭**状态。
   - 只有**资产监控配置**和**基础风险监控配置**需要进行该操作。

   ii. 配置监控参数。

   资产监控配置

参数	说明
监控项	是否选中**子域名发现**。 在导入资产时，可以设置**自动导入子域名**。 如果选中**子域名发现**，则定期对已设置**自动导入子域名**的资产做子域名发现。

参数	说明
监控周期	监控的周期，支持选择**自定义**、**每周**和**每月**。 ■ **自定义**：设置每隔多少天进行一个检测周期。 ■ **每周**：设置每周进行一个检测周期。 ■ **每月**：设置每月进行一个检测周期。
检测时间	检测时间根据**监控周期**结果，设置有所不同。 ■ **监控周期**为**自定义**：设置检测当天的时间范围。 ■ **监控周期**为**每周**：设置哪几天检测和时间范围。 ■ **监控周期**为**每月**：设置哪几天检测和时间范围。 **说明** 例如设置**监控周期**为**每周**，**检测时间**选择**星期一**到**星期天**和0点到24点，则表示7 x 24 小时都进行检测。
端口范围	检测的端口范围，支持**自定义**、**全端口**、**TOP100**和**TOP1000**。 ■ **自定义**：自定义编辑需要扫描的端口。 ■ **全端口**：扫描所有端口。 ■ **TOP100**：扫描Top 100的端口，通过单击**添加**能够设置的自定义端口。 ■ **TOP1000**：扫描Top 1000的端口，通过单击**添加**能够设置的自定义端口。
主机存活检测	用于检测主机是否运行。 默认情况下，使用Ping功能检测。如果主机禁止了Ping功能，则根据Top 20端口和自定义端口检测主机的运行状态。 自定义端口设置：单击**设置**，在**自定义端口**中设置检测端口。

基础风险监控配置

参数	说明
监控项	支持**弱口令**、**常见漏洞**、**基线监控**和**主机合规**等项目。 ■ **弱口令**：对于弱口令，黑客容易猜测到或通过暴力破解，从而获取相关权限。通过检测主机中是否存在弱口令，识别弱口令风险。 ■ **常见漏洞**：常见的漏洞包括Web安全漏洞、CMS应用漏洞等。通过检测常见漏洞，识别漏洞风险，并及时安装漏洞补丁。 ■ **基线监控**：检测主机配置、账号配置等存在的风险点。 ■ **主机合规**：检测主机是否合规。
监控周期	监控的周期，支持选择**自定义**、**每周**和**每月**。 ■ **自定义**：设置每隔多少天进行一个检测周期。 ■ **每周**：设置每周进行一个检测周期。 ■ **每月**：设置每月进行一个检测周期。

参数	说明
检测时间	检测时间根据**监控周期**结果，设置有所不同。 ■ **监控周期**为**自定义**：设置检测当天的时间范围。 ■ **监控周期**为**每周**：设置哪几天检测和时间范围。 ■ **监控周期**为**每月**：设置哪几天检测和时间范围。 **说明** 例如设置**监控周期**为**每周**，**检测时间**选择**星期一**到**星期天**和0点到24点，则表示7 x 24 小时都进行检测。

外部风险监控配置

参数	说明
监控项	支持**代码泄漏**项目。 检测资产中是否存在源代码泄漏的风险。
监控周期	监控的周期，支持选择**自定义**、**每周**和**每月**。 ■ **自定义**：设置每隔多少天进行一个检测周期。 ■ **每周**：设置每周进行一个检测周期。 ■ **每月**：设置每月进行一个检测周期。
检测时间	检测时间根据**监控周期**结果，设置有所不同。 ■ **监控周期**为**自定义**：设置检测当天的时间范围。 ■ **监控周期**为**每周**：设置哪几天检测和时间范围。 ■ **监控周期**为**每月**：设置哪几天检测和时间范围。 **说明** 例如设置**监控周期**为**每周**，**检测时间**选择**星期一**到**星期天**和0点到24点，则表示7 x 24 小时都进行检测。

扫描配置

参数	说明
风险复测	设置风险复测的时间，即每天指定时间对已发现安全风险进行风险复测。
资产扫描速率	设置扫描速度，支持**慢速模式**、**普通模式**、**快速模式**和**极速模式**。
风险扫描速率	设置扫描速度，支持**慢速模式**、**普通模式**、**快速模式**。
UserAgent设置	设置UserAgent属性。

iii. 单击**保存**。

4.8.6.2. 配置基础监控

本文介绍如何设置基础监控。

背景信息

基础监控包括弱口令漏洞监控、运维安全漏洞监控、CMS应用漏洞监控和基线监控。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**配置**。
4. 在**配置**界面，单击**监控配置**。
5. 在**基础监控**页签下，单击**弱口令漏洞监控**，设置弱口令漏洞监控规则。



- 默认情况下，各弱口令监控项使用系统默认的弱口令库。
- 如果需要停用某个监控项，则按照以下步骤操作：

  在**操作**列，单击图标。

- 如果需要启用某个已停用的监控项，则按照以下步骤操作：

  在**操作**列，单击图标。

- 如果需要对单个监控项使用自定义弱口令，则按照以下步骤操作（以**MySQL弱口令漏洞**为例）：

  a. 在**默认弱口令**列，关闭默认弱口令开关，开关状态变更为。

  b. 在**操作**列，单击图标。

c. 在**自定义MySQL弱口令**对话框中，设置自定义的弱口令。



d. 单击**确定**。

- 如果需要对多个监控项使用相同的自定义弱口令，则按照以下步骤操作：

a. 在**默认弱口令**列，关闭默认弱口令开关，开关状态变更为。

> **说明** 对于使用自定义弱口令的监控项，都需要关闭对应的默认弱口令开关。

b. 单击**自定义全局弱口令**。

c. 在**自定义全局弱口令**窗口中，设置自定义的弱口令。

d. 单击**确定**。

6. 单击**运维安全漏洞监控**，设置运维安全漏洞监控。



图示序号	说明
①	开启或关闭**运维安全漏洞监控**功能。 默认情况下建议开启该功能，提高系统的安全性。
②	开启或关闭各监控项。 如果某些监控项不适用于客户的实际业务场景，可以通过此操作关闭该监控项。

7. 单击**CMS应用漏洞监控**，设置CMS应用漏洞监控。



图示序号	说明
①	开启或关闭**CMS应用漏洞监控**功能。 默认情况下建议开启该功能，提高系统的安全性。
②	开启或关闭各监控项。 如果某些监控项不适用于客户的实际业务场景，可以通过此操作关闭该监控项。

8. 单击**基线监控**，设置基线监控。

   新增基线监控项目操作如下：

   i. 单击**添加**。

   ii. 在**添加基线**对话框中，设置新增的基线检查条件。



此处以新增禁止Telnet访问为例，说明如何添加基线。

参数	说明
基线名称	设置基线名称，例如：禁止Telnet访问。
基线规则	设置该基线的检查规则，基线检查时，会扫描主机是否存在指定端口和是否对外开放服务，支持**禁止端口开放**和**禁止服务开放**。 ■ **禁止端口开放**：设置禁止的端口。例如，23。 ■ **禁止服务开放**：设置禁止的服务。例如，Telnet。
基线范围	设置该基线检查适用的资产范围，支持选择**私有IP**或**NatIP**的资产。 选择资产类型，并在下面列表中选中具体的资产。

iii. 单击**确定**。

4.8.6.3. 配置Web监控

本文介绍如何设置Web监控。

背景信息

Web监控可以设置Web漏洞的监控项，同时也能够设置网站爬虫等限制条件。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**配置**。
4. 在**监控配置**界面，单击**WEB监控**页签，查看已创建的规则列表。



> **说明** **默认规则**为系统创建的，只能查看详情，不能进行修改和删除。

5. 新增Web监控规则。
   i. 单击**添加规则**。

ii. 在**添加Web监控规则** 页面，设置规则参数。

参数	说明
规则名称	填写Web监控规则的名称。
监控周期	设置监控的周期，支持选择**自定义**、**每周**和**每月**。 ■ **自定义**：设置每隔多少天进行一个检测周期。 ■ **每周**：设置每周进行一个检测周期。 ■ **每月**：设置每月进行一个检测周期。
检测时间	检测时间根据**监控周期**结果，设置有所不同。 ■ **监控周期**为**自定义**：设置检测当天的时间范围。 ■ **监控周期**为**每周**：设置哪几天检测和时间范围。 ■ **监控周期**为**每月**：设置哪几天检测和时间范围。 **说明** 例如设置**监控周期**为**每周**，**检测时间**选择**星期一**到**星期天**和0 点到24 点，则表示7 x 24 小时都进行检测。
监控选项	选择需要监控的Web漏洞类型，支持**全选**、**反选**和**清空**操作。
UserAgent	设置HTTP请求包的UserAgent字段。 UserAgent字段用于识别发起请求的用户代理软件的应用类型、操作系统、软件开发商以及版本号。
Cookies	设置Cookies参数。
重点页面	设置需要重点监控的Web目录或页面。
排除页面	设置不需要监控的Web目录或页面。
爬虫深度	设置爬虫抓取的深度，取值为**10**、**15**、**30**。
爬虫URL数	设置爬虫抓取的URL数量，取值为**500**、**1000**、**2000**。
扫描频率	设置Web监控扫描的频率，取值为**10 请求每秒**、**15 请求每秒**。

iii. 单击**确定**。

6. 管理已创建的规则。

操作按钮	说明
	修改该规则。
	删除该规则。

操作按钮	说明
批量删除	如果需要删除多个规则，则选择多个规则，单击**批量删除**。

4.8.6.4. 配置白名单

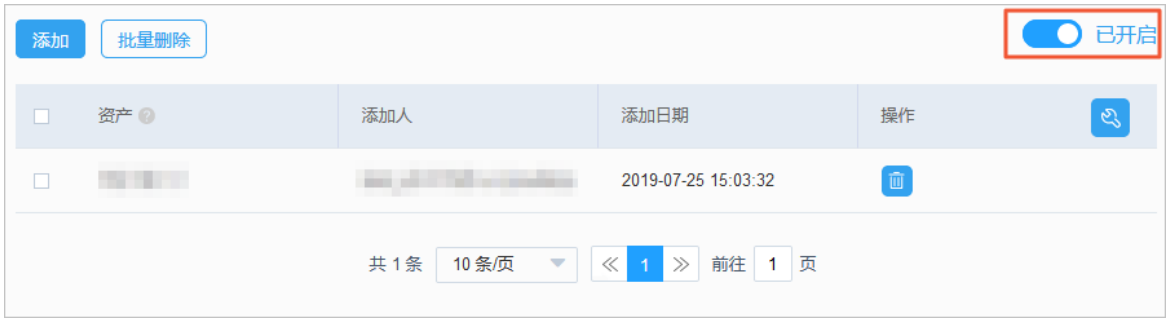
本文介绍如何设置监控白名单。

背景信息

系统将不会对加入到白名单中的资产进行漏洞扫描，在设置白名单前，请确认加入资产的安全性。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**配置**。
4. 在配置界面，单击**监控配置**，单击**白名单**页签，查看已添加的白名单资产列表。



> **说明** 默认启用白名单功能，如果不需要使用白名单功能，则单击右上角的白名单切换开关，切换至**已关闭**状态。

5. 添加新的白名单。
   i. 单击**添加**。

ii. 在**添加白名单**对话框，设置白名单。



- **白名单**选择**资产分组**方式：在第二个下拉菜单中选择分组，则该分组的资产会放入白名单中。
- **白名单**选择**自定义**方式：在下面输入框中，输入需要加入白名单的IP或URL。

iii. 单击**确定**。

6. 管理白名单列表。
   - 删除单个白名单：

     在单个资产的**操作**栏，单击图标，将单个资产从白名单列表中删除。

   - 批量删除白名单：

     选中多个资产，单击**批量删除**，将多个资产从白名单列表中删除。

4.8.6.5. 配置扫描引擎（私有资产）

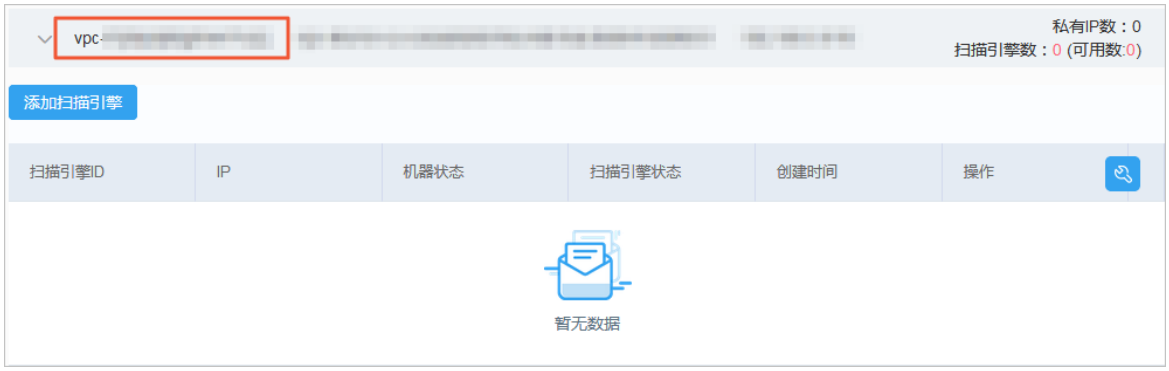
本文介绍如何为VPC配置扫描引擎。

背景信息

只有通过给VPC授权扫描引擎，VPC对应的资产才能够进行漏洞扫描。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**漏洞扫描**。
3. 在左侧导航栏，单击**配置**。
4. 在**配置**页面，单击**扫描引擎管理**页签。
5. 单击**私有资产**页签。
6. 单击需要进行漏洞扫描的VPC名称。



7. 单击**添加扫描引擎**。
8. 在**添加扫描引擎**对话框中，通过**vswitch**下拉菜单选择VPC的虚拟交换机。
9. 单击**确定**。

4.9. 安全报告

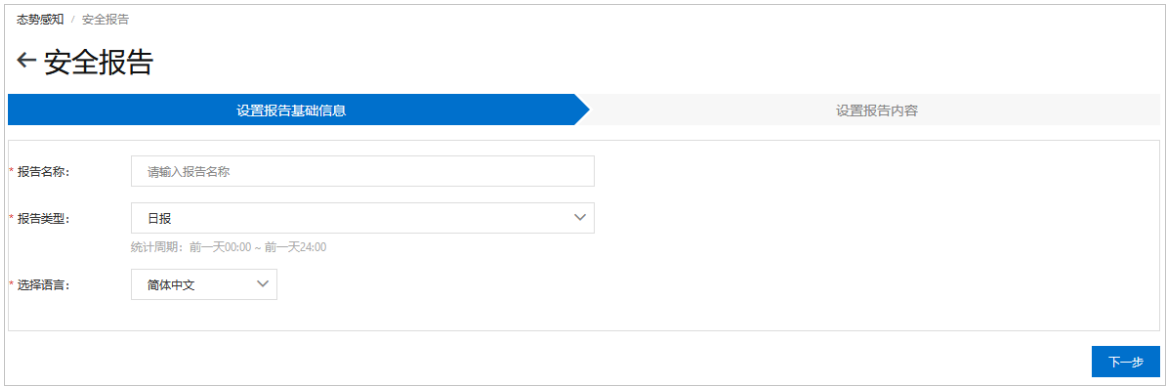
您可以通过自定义报告内容、报告展示的数据类型和接收人邮箱地址，实现安全报告的自定义，更好地满足您对于资产安全状况数据的需求。本文介绍如何创建安全报告。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**安全管理**区域单击**态势感知**。
3. 在左侧导航栏，单击**安全报告**。
4. 在**安全报告**页面，单击**创建新报告**。

> 注意 云盾安全中心除默认已创建的安全日报，最多支持创建9个安全报告。

5. 在**设置报告基础信息**页签中，配置安全报告的基本信息。



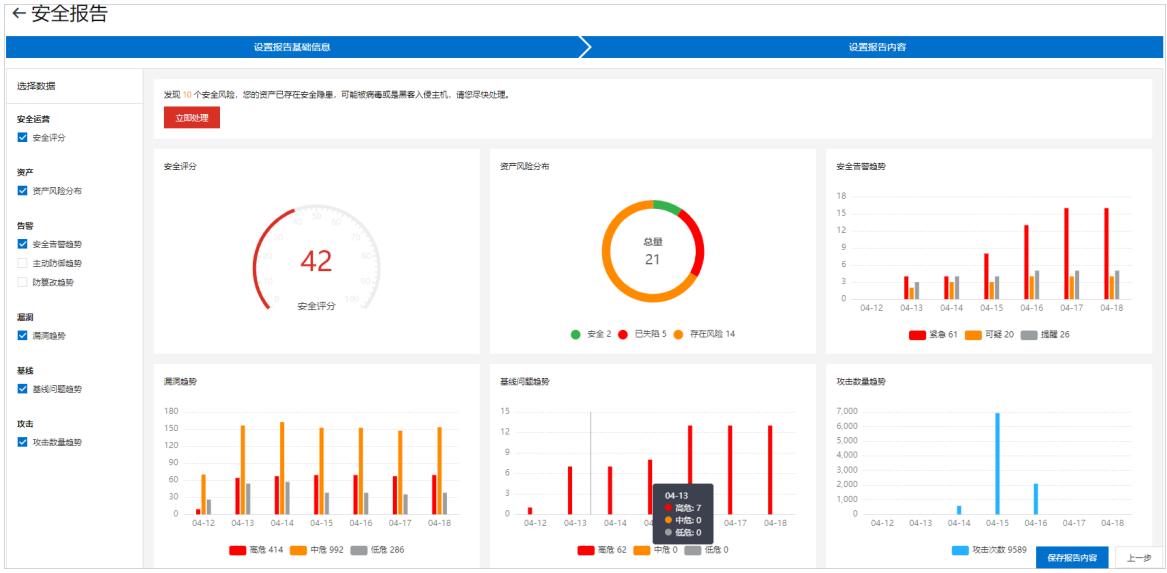
您可以参考以下说明配置安全报告参数：

- **报告名称**：手动输入安全报告的名称。
- **报告类型**：单击下拉框选择创建报告的类型，可选*日报*、*周报*、*月报*和*自定义周期*报告。

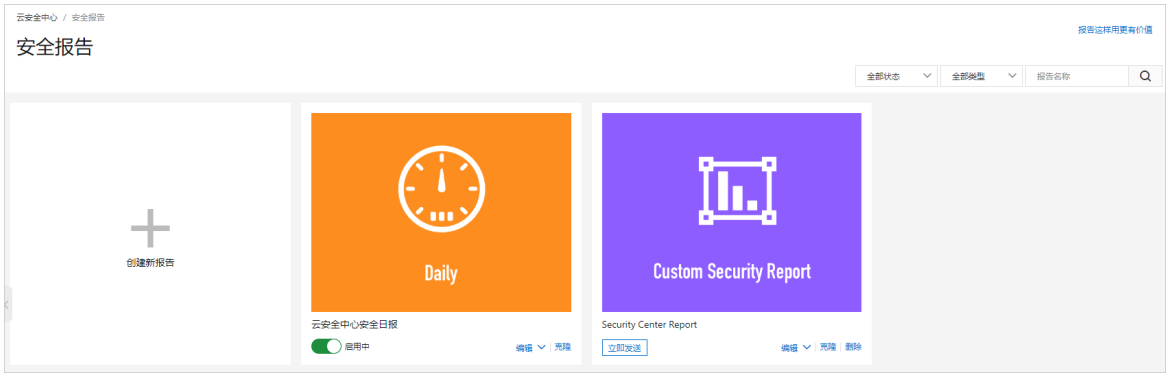
  如果选择*自定义周期*，您需要在**统计周期**中选择该自定义安全报告统计的周期。
- **选择语言**：单击下拉选框，选择安全报告的语言，可选**简体中文**或者**English**。

6. 单击**下一步**。

7. 在**设置报告内容**页签中，选中需要在报告中展示的数据，可以选择资产、告警、漏洞、基线、攻击、安全运营相关统计数据。



8. 单击右下角**保存报告内容**，完成报告的创建。
您可在**安全报告**页面查看到您新建的报告。



5.网络流量检测与响应

5.1. 查看流量趋势

本文介绍如何查看网络流量趋势、入口流量统计和出口流量统计。

背景信息

安全管理员通过分析流量趋势，可以定位流量速率、流量的高峰和低谷时段等分布规律；同时通过查看Top 5流量的IP，甄别恶意的IP访问。

操作步骤

1.
2. 在控制台右上方，单击**安全**，选择**网络安全 > 流量安全监控**。
3. 在 **流量趋势**页面，单击右上角的时间（**近1小时**、**近24小时**或**近7天**），选择时间范围。
4. 查看网络流量信息。
   - 网络流量趋势

     查看在选择的时间段内的网络流量趋势，包括入流量的bps和出流量的bps。
   - 网络入方向

     查看网络入方向的会话、应用和Top访问目的IP等统计信息。
   - 网络出方向

     查看网络出方向的会话、应用和Top访问源IP等统计信息。
5. （可选）单击图标，将流量趋势信息导出为PDF。

5.2. 查看互联网边界流量

本文介绍如何查看互联网边界的流量，您可以通过这些流量信息了解网络安全情况。

前提条件

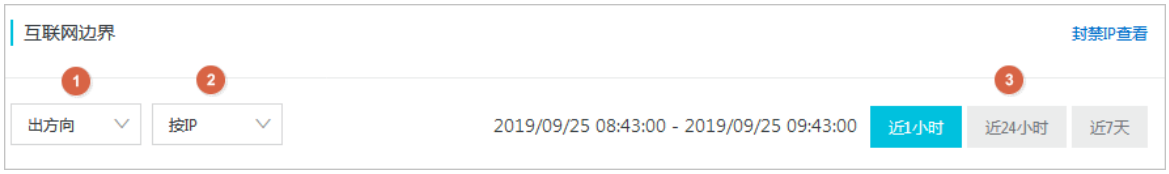
在使用互联网边界流量功能前，您需确认已采购和部署**流量安全监控（ISW）-用于互联网边界出入流量的全流量审计和分析管控**。

背景信息

通过流量信息，您可以识别出互联网异常流量，并通过封禁功能阻断恶意访问来源。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**互联网边界**。
4. 在左侧导航栏，选择**网络安全 > 流量分析 > 互联网边界**。
5. 设置流量筛选条件。



设置位置	筛选条件说明
①	设置查看的流量方向，支持*入方向*和*出方向*。 ○ *入方向*：从互联网访问内网。 ○ *出方向*：从内网访问互联网。
②	设置*按IP*和*按应用*查看互联网边界流量 。
③	设置查看的时间范围，支持*近1小时*、*近24小时*和*近7天*。

6. 查看互联网边界流量详细信息。
   - **流量统计**信息



     - 在**IP访问情况**中查看**源IP数**、**目的IP数**、**应用数**和**流量风险**。
     - 在右侧流量图中，查看**均值流量**、**峰值流量**和流量趋势。

   - **流量列表**



     在**流量列表**中查看流量的详细情况。

7. 在**流量列表**中，查看目标IP的异常流量。

- 当流量选择*入方向*时，在**流量列表**的**目的IP维度**页签中查看异常流量信息。
- 当流量选择*出方向*时，在**流量列表**中查看异常流量信息。

8. 通过封禁功能，阻断恶意访问来源。

   手工封禁功能操作步骤，具体请参见一键封禁。

9. 在**互联网边界**页面，单击右上角的**封禁IP查看**，查看被封禁的IP列表。

5.3. 查看内网边界流量

本文介绍如何查看内网边界的流量，您可以通过这些流量信息了解网络安全情况。

前提条件

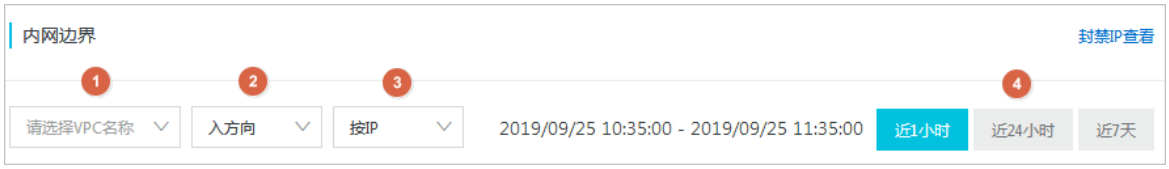
在使用内网边界流量功能前，您需确认已采购和部署**流量安全监控（CSW）- 用于IDC和VPC的内网专线出入流量的全流量审计和分析管控**。

背景信息

通过流量信息，您可以识别出内网异常流量，并通过封禁功能阻断恶意访问来源。

操作步骤

1.
2. 在控制台右上方，单击**安全**，选择**网络安全 > 流量安全监控**。
3. 在左侧导航栏，选择**内网边界**，在**内网边界**页面设置流量筛选条件。



设置位置	筛选条件说明
①	在下拉框中选择VPC实例名称。
②	设置查看的流量方向，支持*入方向*和*出方向*。 ○ *入方向*：从互联网访问内网。 ○ *出方向*：从内网访问互联网。
③	设置*按IP*和*按应用*查看内网边界流量 。
④	设置查看的时间范围，支持*近1小时*、*近24小时*和*近7天*。

4. 查看内网边界流量详细信息。
   - **流量统计**信息
     - 在**IP访问情况**中查看**源IP数**、**目的IP数**、**应用数**和**流量风险**。
     - 在右侧流量图中，查看**均值流量**、**峰值流量**和流量趋势。
   - **流量列表**
     - 在**流量列表**中按**源IP维度**、**目的IP维度**查看流量的详细情况。

- 如果以**按IP**条件筛选，在**流量列表**中可以查看相关IP的异常流量。

5.

6. 在**内网边界**页面，单击右上角的**封禁IP查看**，查看被封禁的IP列表。

5.4. 管理网络抓包任务

本文主要介绍如何创建网络抓包任务。通过网络抓包功能捕获指定IP和端口的网络数据包、分析数据包内容，帮助您定位网络故障和分析攻击行为，从而识别出网络通信的安全风险。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**网络抓包**。
4. 在**网络抓包**页面，单击**新建抓包任务**。
5. 在**新建抓包任务**面板，配置任务参数，单击**确认**。



参数	说明
任务名	设置抓包任务名称。建议您输入任务目的等信息。
最大字节数	设置抓取数据包的最大字节数。如果数据包超过该字节数，则丢弃超出部分。
时长（s）	设置抓包的最长时间。单位：秒。

参数	说明
协议	设置抓包的协议类型。可选项： ○ 全部 ○ TCP ○ UDP ○ ICMP
IP配置类型	选择IP配置类型。可选项：IPV4 、IPV6。
方向	设置过滤的流量方向。可选值：双向、In、Out。
IP	设置过滤的IP。
端口	设置过滤的端口。

执行结果

您可在**网络抓包**页面，查看新建的抓包任务和任务状态信息。



5.5. 日志检索

本文介绍如何检索和查看日志。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**日志检索**。
4. 在**日志检索**页面，设置搜索条件。

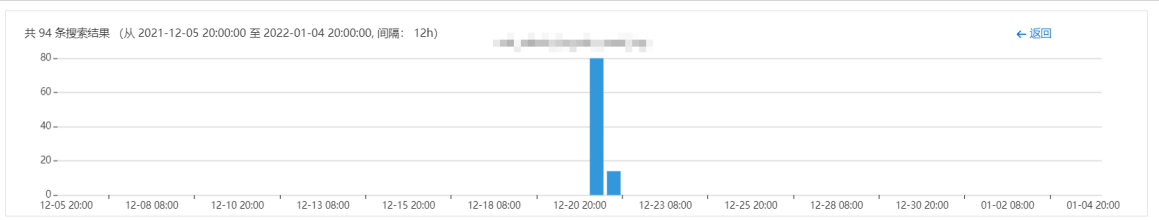


搜索项	说明
时间	设置检索日志的时间段。可选值：最近一小时、最近4小时、今天、最近7天、最近14天、最近30天、自定义。
全部部门	选择检索日志的所属部门。

搜索项	说明
日志类型	选择检索日志的类型，分为**安全日志事件**和**全流量日志**两大类。
搜索模板	选择检索日志的模板。模板是先前搜索条件保存的模板。
请输入内容	输入日志的相关内容。

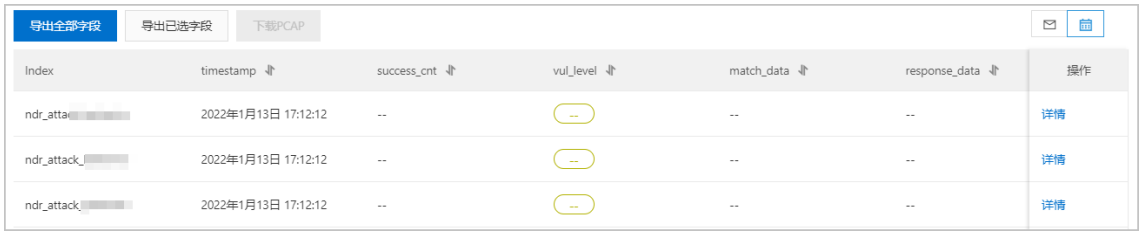
5. 单击**搜索**图标，查看搜索结果。
   - **清除**：如果不需要原来设置的搜索条件，单击**清除**，搜索条件回到初始状态。
   - **保存**：如果以后需要重用这个搜索条件，单击**保存**，设置**名称**进行保存，则保存了一个搜索模板。

   根据查询条件，系统会以柱状图的形式为您展示平台日志。您可以通过柱状图，了解指定时间范围内不同时间的日志数量。



在日志检索页面下方，您可以查看查询到的日志详细信息。单击日志列表的参数，可以直接将参数加到搜索条件。

- 选择日志列表的展示字段：在日志检索页面的左下方选择展示字段。



- 导出检索日志的全部字段：单击**日志检索**页面上的**导出全部字段**，可以导出搜索出的日志的全部字段。全部字段包含**展示字段**和**可选字段**，即**日志检索**页面左下方列的所有字段。
- 导出检索日志的已选字段：单击**日志检索**页面上的**导出已选字段**，可以导出按条件搜索出的日志的展示字段。
- 查看日志详情：单击日志列表操作列的**详情**，可以查看当前行的日志详细信息。
- 查看字段信息：单击日志页面右上角的**帮助文档**，可以查看日志字段说明。
- 字段参数解码：单击日志页面右上角的**解码小工具**，可以将各编码参数转换成别的形式的参数。

5.6. 攻击者画像

攻击者画像从攻击者的视图，展示攻击者的基础信息、威胁情报、攻击手法、攻击目标、攻击过程，并进行统一的分析展示。本文介绍如何查看攻击者画像。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**攻击者画像**。
4. 在**攻击者画像**页面，设置搜索条件。

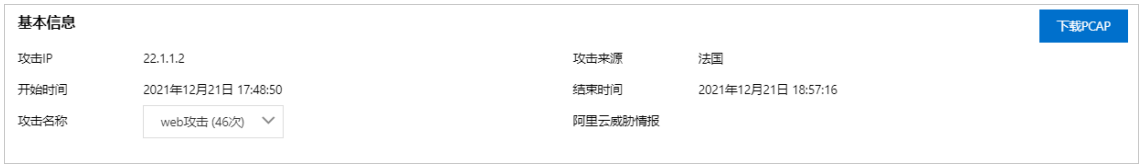


搜索项	说明
时间	设置攻击时间段。可选值：**最近一小时**、**最近4小时**、**今天**、**最近7天**、**最近14天**、**最近30天**、**自定义**。
攻击结果	选择攻击结果的类型，攻击结果有**尝试**和**成功**两种类型。
威胁等级	选择攻击的威胁类型，可选值有：**低危**、**中危**、**高危**。
请输入攻击IP	输入攻击的IP地址。

5. 在**列表**页面，查看符合搜索条件的攻击列表。



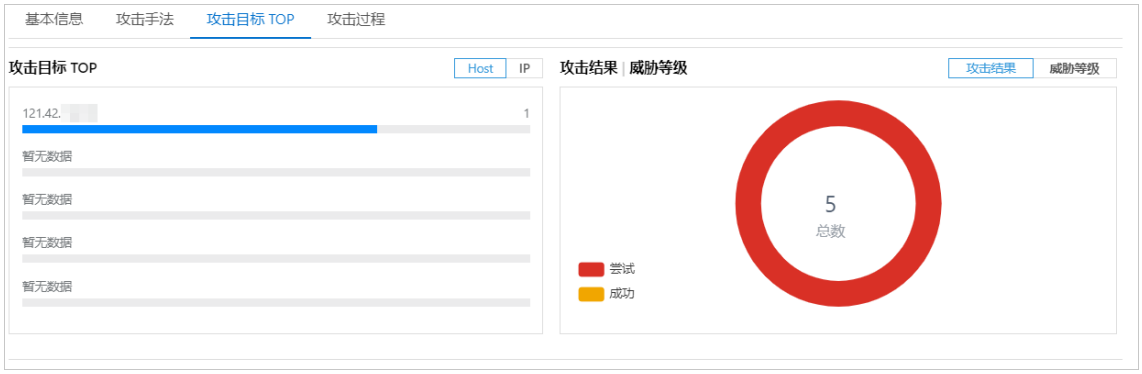
6. 单击**列表**页面的目标攻击，查看该目标攻击信息。
   - 单击**基本信息**页签，您可以查看攻击的基本信息。



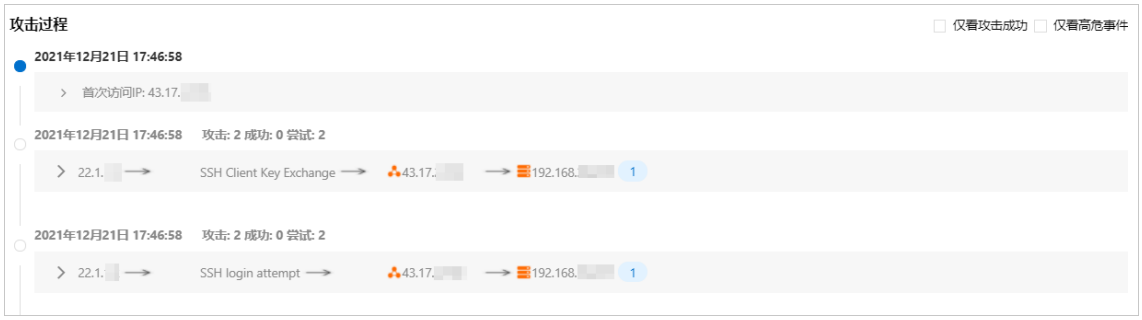
   - 单击**攻击手法**页签，您可以查看攻击的详细记录。



   - 单击**攻击目标TOP**页签，您可以查看受攻击数为前五的攻击目标HOST、IP数量，还可以查看尝试攻击和攻击成功的攻击数量、不同威胁等级的攻击数量。



- 单击**攻击过程**页签，查看攻击的详细过程。



5.7. 威胁检测

5.7.1. 威胁检测

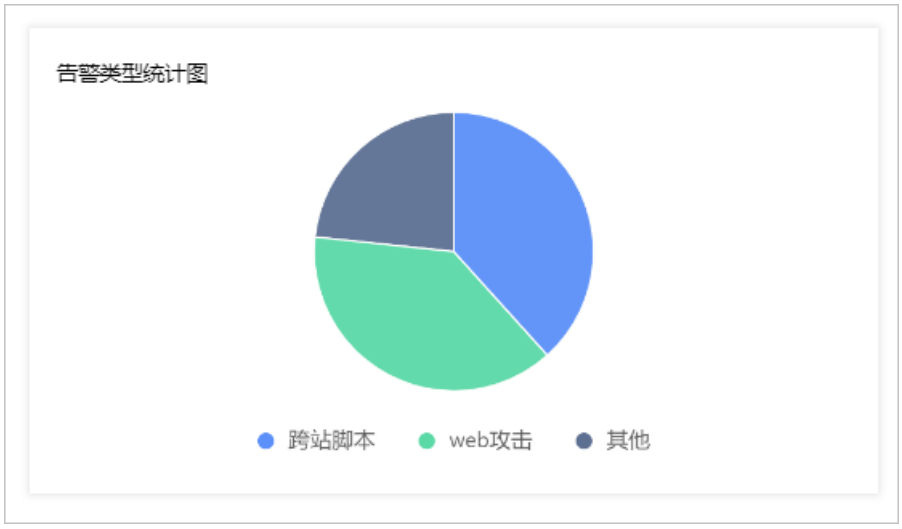
本文介绍如何查看威胁检测的信息记录。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**威胁检测**。
4. 在**威胁检测**页面，单击**威胁检测**。
5. 在**威胁检测**页签，设置查询条件。
6. 单击**查询**，查看查询结果。

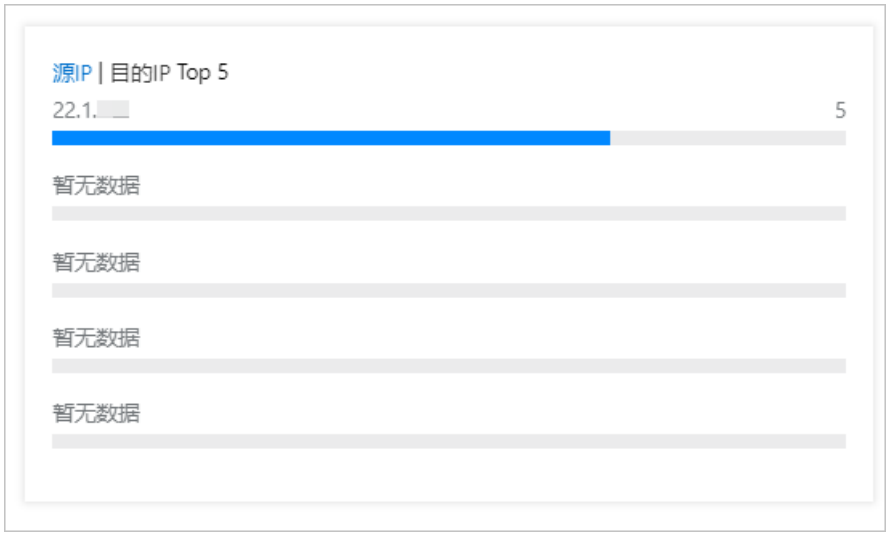
   如果不需要原来设置的搜索条件，单击**重置**，搜索条件回到初始状态。

   根据查询条件，系统会以图表的形式为您进行攻击分析。

   - 您可以通过告警类型统计图，了解不同告警类型的攻击数量。



- 您可以通过二维条形图，了解Top5的源IP、目的IP的攻击数量。



- 您可以通过告警趋势图，了解指定时间范围内攻击的数量趋势。
- 您可以在攻击防护页面的下方查看攻击列表，攻击列表可以查看详细攻击信息。



  - 设置自定义列：单击自定义列，可以选择需要在告警列表中展示的列。列表默认展示的列为：**攻击时间**、**攻击名称**、**部门**、**攻击源**、**被攻击资产**、**攻击payload**、**风险等级**、**攻击结果**、**防护状态**。
  - 查看攻击详情：单击**详情**，查看攻击的**基本信息**、**规则详情**、**原始告警列表**。
  - 设置攻击标签：单击**标签**，设置攻击的自定义标签。

- 设置攻击处置：单击**处置**，设置攻击处置。支持的处置操作包括：**封禁**、**加入白名单**、**忽略**。



- **封禁**：通过网络层访问控制策略对攻击IP进行阻断。

参数	说明
源IP	告警中的攻击源。
目的IP	告警中的被攻击资产的IP地址。
目的端口	攻击的目的端口。
生效时间	支持设置处置操作的生效时间：**一天**、**一周**、**一个月**、**自定义**、**永久**。

- **加入白名单**：将IP地址加入白名单，该IP为源或目的的攻击行为不再产生告警。加入白名单后会记录到**白名单列表**里，在**白名单列表**可以删除和新增白名单。
- **忽略**：忽略单条告警，后续攻击依旧会产生告警。

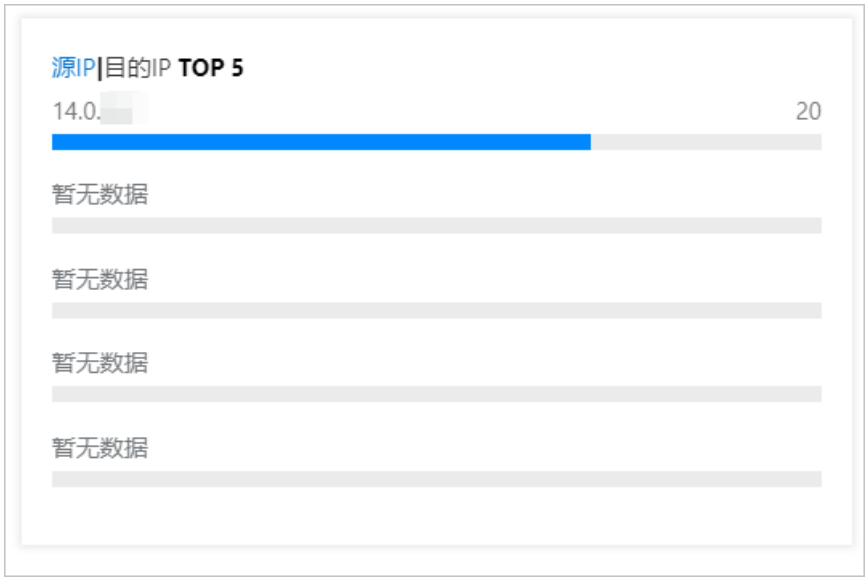
攻击列表中的防护状态，展示用户执行过的处置操作。默认未处置。用户执行任意处置操作后，更新防护状态。防护状态与处置操作一一对应，设置**封禁**则显示**已封禁**、设置**加入白名单**则显示**已加白**、设置**忽略**则显示**已忽略**。

- 导出攻击列表：单击**导出全部记录**，导出查询到的攻击列表。

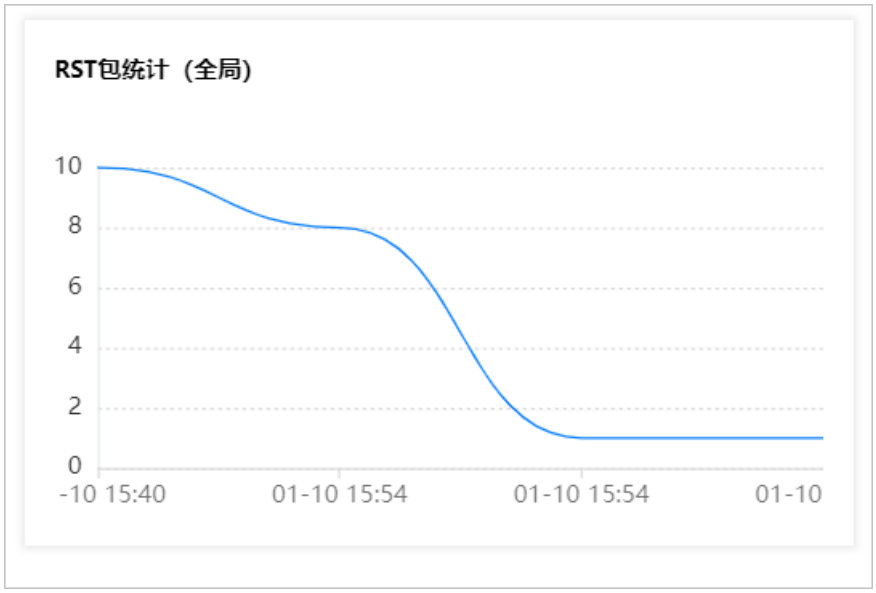
5.7.2. 查看封禁日志

封禁日志是命中封禁策略的流量产生的日志。本文介绍了如何查看封禁日志。

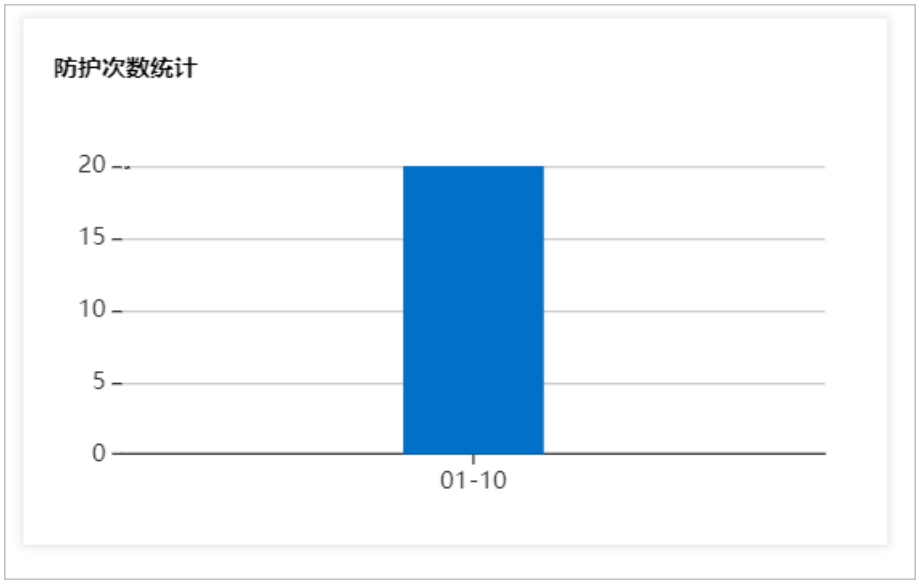
1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**威胁检测**。
4. 在**威胁检测**页面，单击**封禁日志**。
5. 在**封禁日志**页签，设置查询条件。
6. 单击**查询**。
   - 您可以通过二维条形图，了解时间周期内Top 5的源IP、目的IP的攻击数量。



   - 您可以通过二维折线图，了解不同时间的RST包数量。



   - 您可以通过**防护次数统计**图，了解指定时间的攻击防护次数。



- 您可以在**封禁日志**页面的下方查看封禁日志列表，在封禁日志列表可以查看封禁日志的详细信息。



在封禁日志列表上方，您可以单击**导出全部记录**，导出记录的攻击。在在封禁日志列表的**操作**列，您可以设置**策略动作**，**策略动作**有**阻断**、**加白**、**观察**三种。选中多个记录，您还可以进行批量设置策略动作。

- **阻断**：系统检测到符合封禁策略的流量后产生告警并对访问进行阻断。
- **观察**：系统检测到符合封禁策略的流量后产生告警但不阻断流量。
- **加白**：对加白的IP地址流量不产生告警。

5.8. 行为分析

5.8.1. 加密流量分析

加密流量分析可以通过行为特征分析的方式发现可疑的加密通信行为。本文介绍了如何查看加密流量分析的数据。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**行为分析**。
4. 在**行为分析**页面，单击**加密流量分析**。
5. 在**加密流量分析**页签，设置搜索条件。

   您可以通过选择**时间**、**部门**、**源IP**、**目的IP**、**攻击工具类型**来进行查询。



6. 单击**查询**，查看查询结果。

根据查询条件，您可以通过以下图表查看加密流量分析数据：

- **加密流量类型分析**
- **攻击工具类型分析**
- **源IP|目的IP Top5**

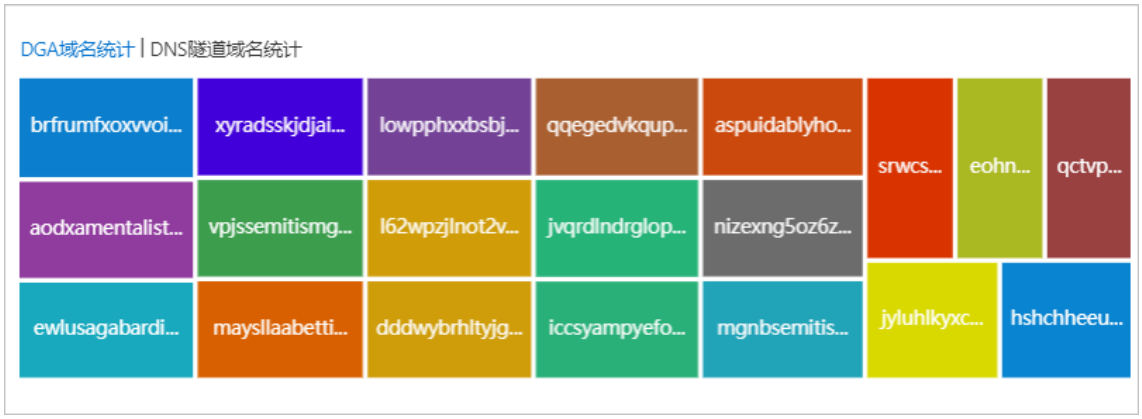
5.8.2. DNS行为分析

DNS行为分析可以通过行为特征分析可疑DNS域名，发现可疑行为，本文介绍了如何查看DNS行为分析的数据。

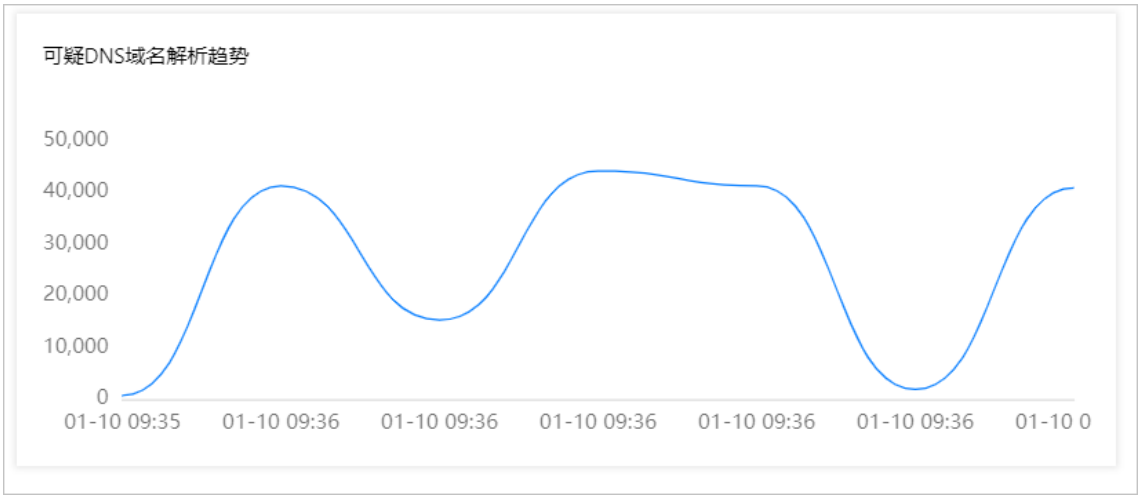
1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**行为分析**。
4. 在**行为分析**页面，单击**DNS行为分析**。
5. 在**日志检索**页面，设置搜索条件。

   您可以根据需要，设置时间、部门、域名、源IP、异常类型进行查询。
6. 单击**查询**。

   根据查询条件，系统会以图表的形式为您分析DNS行为。
   - 您可以通过查看**DGA域名统计**，获取DGA域名，通过查看**DNS隧道域名统计**，获取DNS隧道域名。

   - 您还可以通过**可疑DNS域名解析趋势**图，查看可疑DNS域名解析趋势，了解指定时间范围内不同时间的DNS行为次数。



- 您可以在**DNS行为分析**页签下方的DNS行为列表，查看DNS行为信息。



在DNS行为列表，您还可以进行如下操作：

- 查看行为详情：单击DNS行为列表**操作**列的**详情**，可以查看当前行行为的详细信息。
- 行为加白：单击DNS行为列表**操作**列的**加白**，可以将当前行行为加入白名单。在**白名单列表**中，可以查看加白的行为。
- 设置DNS隧道规则：单击**DNS隧道规则**，可以设置DNS隧道行为检测规则。

5.9. 配置策略

5.9.1. 配置网络层策略

本文介绍了如何新增网络层策略和查看网络层策略。

新增网络层策略

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 在**网络层策略**页签，单击**新增策略**。
5. 在新增策略页面，设置参数。



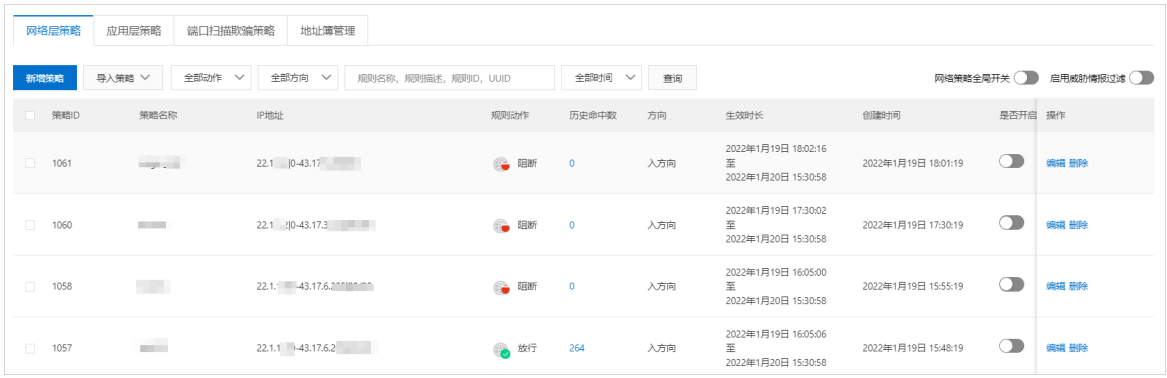
参数	说明
策略名称	设置策略的名称。
策略描述	设置策略的信息描述。
方向	策略的方向。
策略类型	设置策略的类型，可选值：**仅源IP**、**仅目的IP**、**源IP**、**目的IP/端口**。
规则	设置策略规则。可选值：**手动输入**、**导入文件**、**地址簿**。可设置多个策略。

参数	说明
是否开启	通过开关设置是否可以实行策略。
动作	选择策略的行为动作，可选值：**放行**、**观察**、**阻断**。
生效时间	选择策略的生效时长，可选值：**永久生效**、**一天**、**一周**、**一个月**、**自定义**。

6. 单击**确定**。
   新增的策略会显示在在**网络层策略**页签下方的策略列表。

查看网络层策略

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 在**网络层策略**页签，查看策略列表。



在策略列表，您还可以进行如下操作：

- 搜索策略：在策略列表上方，您可以选择策略的规则动作、方向，输入规则名称、规则描述、规则ID、UUID信息，设置策略创建时间进行搜索。
- 选择是否开启策略：通过策略列表的**是否开启**列的开关进行设置。
- 编辑策略：在策略列表的**操作**列，单击**编辑**，您可以编辑策略信息。
- 删除策略：在策略列表的**操作**列，单击**删除**，您可以删除所在行的策略。
- 启用网络策略全局：在策略列表的上方，单击**网络策略全局**开关。
- 启用威胁情报过滤：在策略列表的上方，单击**启用威胁情报过滤**开关。启用威胁情报对网络流量中的恶意IP进行过滤。威胁情报匹配的流量默认将阻断。

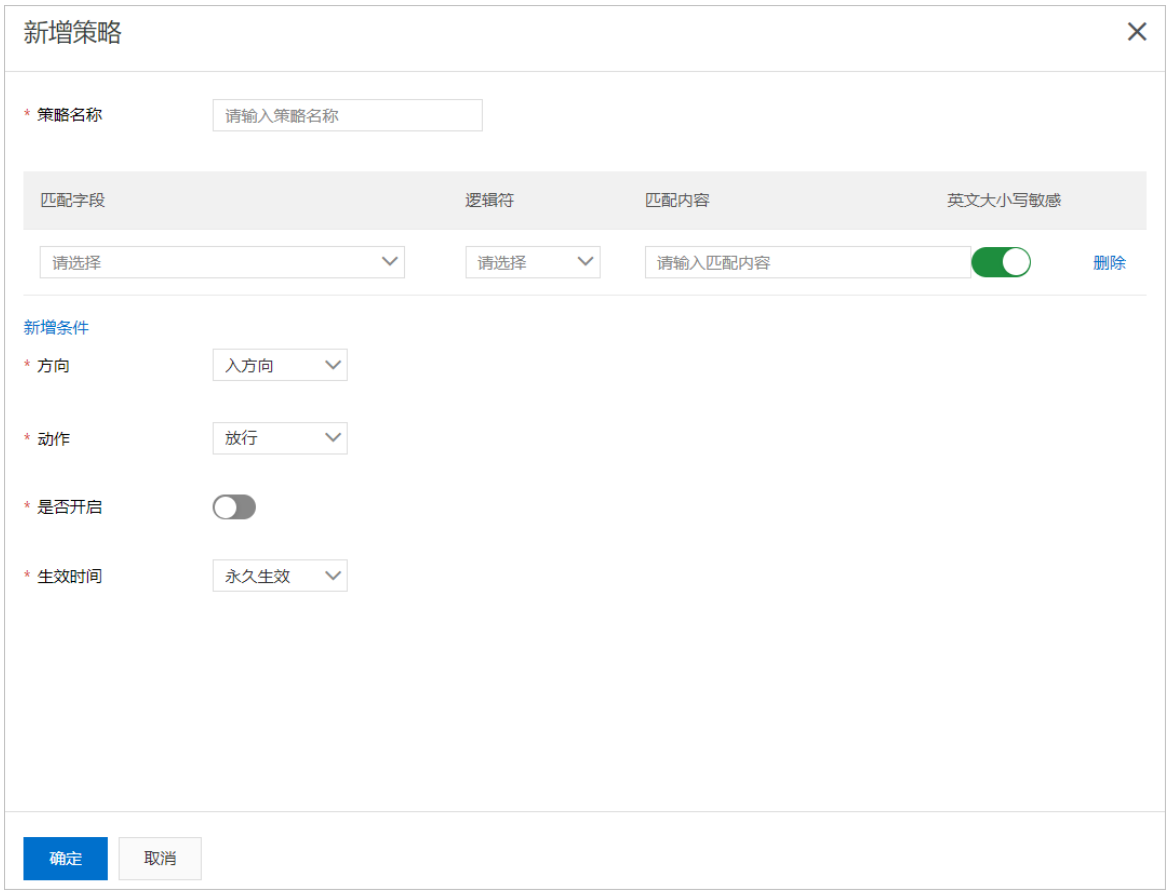
5.9.2. 配置应用层策略

本文介绍了如何新增应用层策略、查看应用层策略和查看WEB应用检测配置。

新增应用层策略

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。

4. 单击**应用层策略**。
5. 在**应用层策略**的**HTTP自定义策略**页签，单击**新增策略**。
6. 在新增策略页面，设置参数。



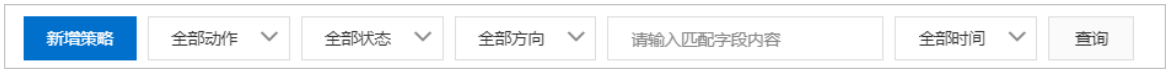
参数	说明
策略名称	设置策略的名称。
方向	选择策略的方向，可选值：**入方向**、**出方向**。
匹配条件	策略的核心内容，添加多个匹配条件，仅当有符合匹配条件的流量发起时，才通过策略进行**放行**、**观察**、**阻断**。通过选择**匹配字段**、**逻辑符号**、**匹配内容**和设置**英文大小写敏感**来添加匹配条件。
动作	选择策略的行为动作，可选值：**放行**、**观察**、**阻断**。
是否开启	通过开关设置是否可以实行策略。
生效时间	选择策略的生效时长，可选值：**永久生效**、**一天**、**一周**、**一个月**、**自定义**。

7. 单击**确定**。
   新增的策略会显示在在**HTTP自定义策略**页签下方的策略列表。

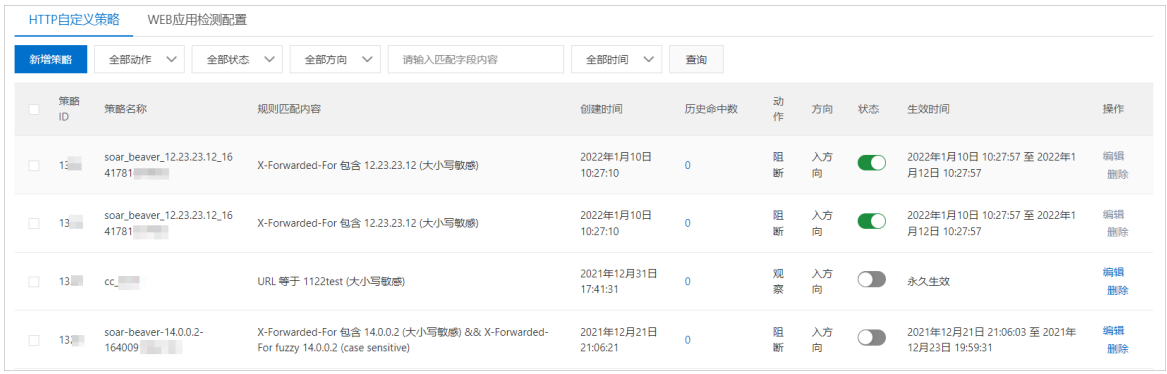
查看应用层策略

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 单击**应用层策略**。
5. 单击**HTTP自定义策略**页签。
6. 在**HTTP自定义策略**页签，设置搜索条件。

   您可以通过选择策略动作、状态、方向、时间来进行策略搜索。



7. 单击**查询**。
8. 在**HTTP自定义策略**页签，查看策略列表。



   在策略列表，您还可以进行如下操作：

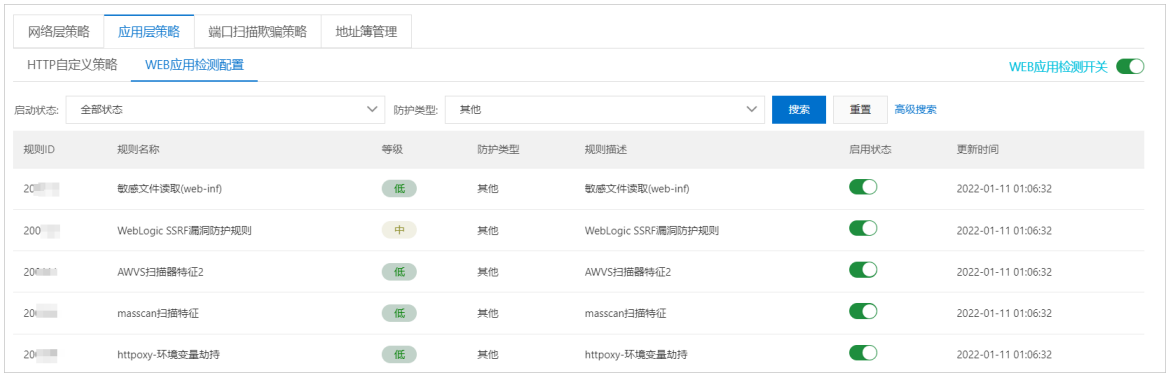
   - 编辑策略：在策略列表的**操作**列，单击**编辑**，您可以编辑策略信息。
   - 删除策略：在策略列表的**操作**列，单击**删除**，您可以删除所在行的策略。

查看WEB应用检测配置

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 单击**应用层策略**。
5. 单击**WEB应用检测配置**页签。
6. 在**WEB应用检测配置**页签，设置**启动状态**和**防护类型**搜索条件。



7. 单击**搜索**，查看WEB应用检测配置列表。



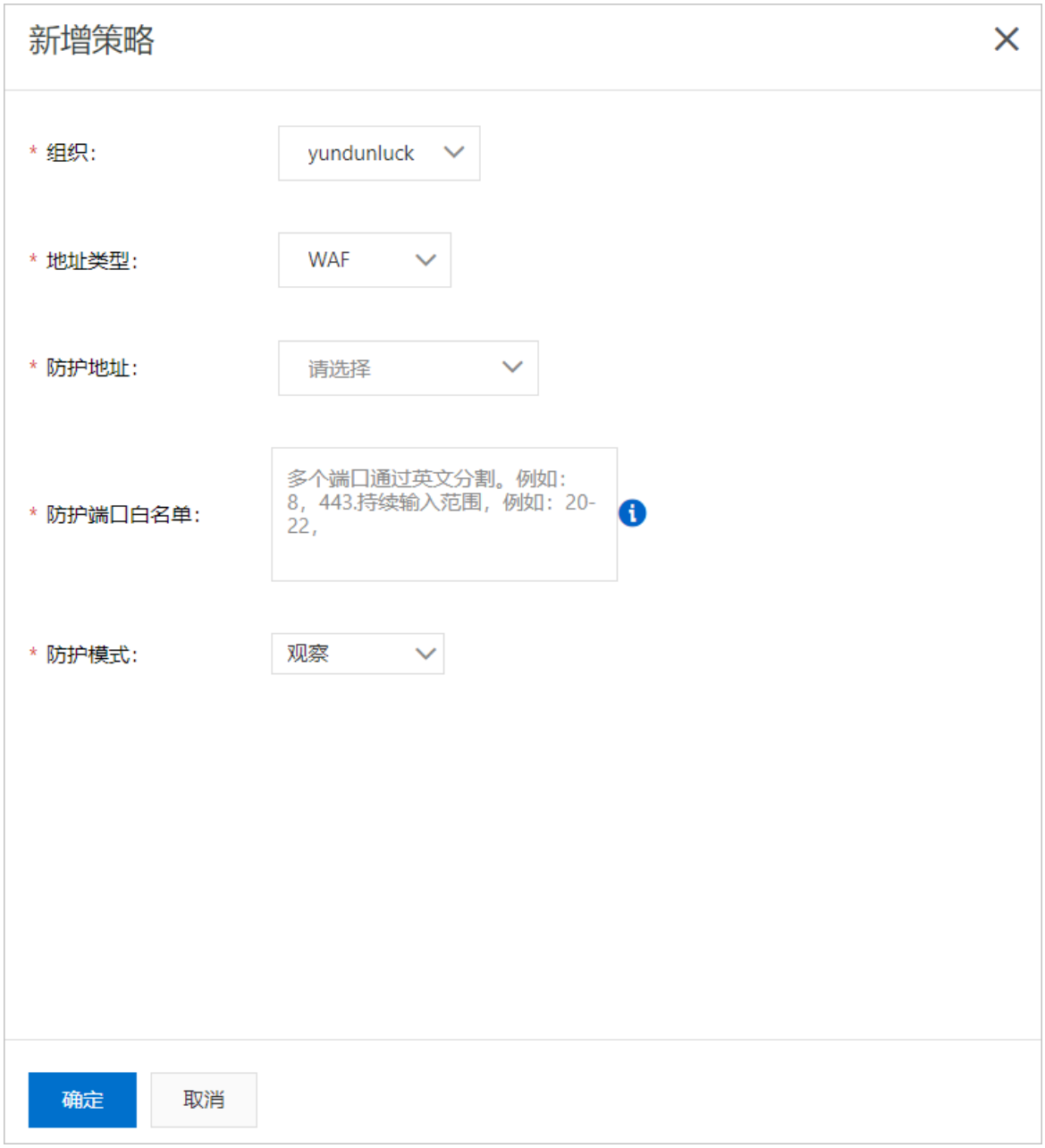
- 设置单条WEB应用配置检测状态：打开WEB应用配置检测列表的**启用状态**列开关，表示**启动状态**为**生效中**，关闭表示**已失效**。
- 设置全局WEB应用检测状态：打开WEB应用配置检测列表上方的**WEB应用检测开关**开关，启用检测。关闭开关，停止检测。

5.9.3. 配置端口扫描欺骗策略

端口扫描欺骗策略通过欺骗攻击者原本不存在的端口存活，让攻击者发起攻击尝试，从而暴露恶意攻击行为。本文介绍了如何配置端口扫描欺骗策略。

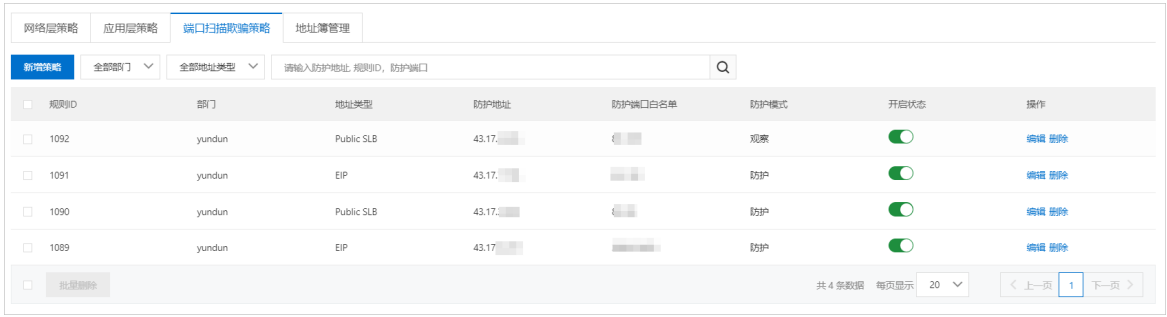
背景信息

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 单击**端口扫描欺骗策略**。
5. 在**端口扫描欺骗策略**页签，单击**新增策略**。
6. 在新增策略页面，设置参数。



参数	说明
组织	当前平台的组织列表。
地址类型	通过安全组件的接口，获取租户已经配置的 IP地址和端口。可选值：**WAF**、**Public SLB**、**EIP**、**自定义**。
防护地址	获取地址列表。
防护端口白名单	填写防护端口白名单。白名单以内的端口不会进行扫描欺骗，白名单以外的其他全部端口则开启扫描欺骗。
防护模式	选择防护模式，可选值：**观察**、**防护**。**观察**表示产生告警，不拦截。**阻断**表示产生告警，且拦截。

7. 单击**确定**。



在策略列表中，您还可以进行如下操作：

- 搜索策略：在策略列表上方，选择策略动作、状态、方向、时间进行搜索。
- 编辑策略：在策略列表的**操作**列，单击**编辑**，您可以编辑策略信息。
- 删除策略：在策略列表的**操作**列，单击**删除**，您可以删除所在行的策略。
- 批量删除策略：您选中需要删除的策略前的复选框，单击**批量删除**。
- 设置策略状态：打开策略列表的**开启状态**列的开关，启用策略。关闭策略列表的**开启状态**列的开关，停用策略。

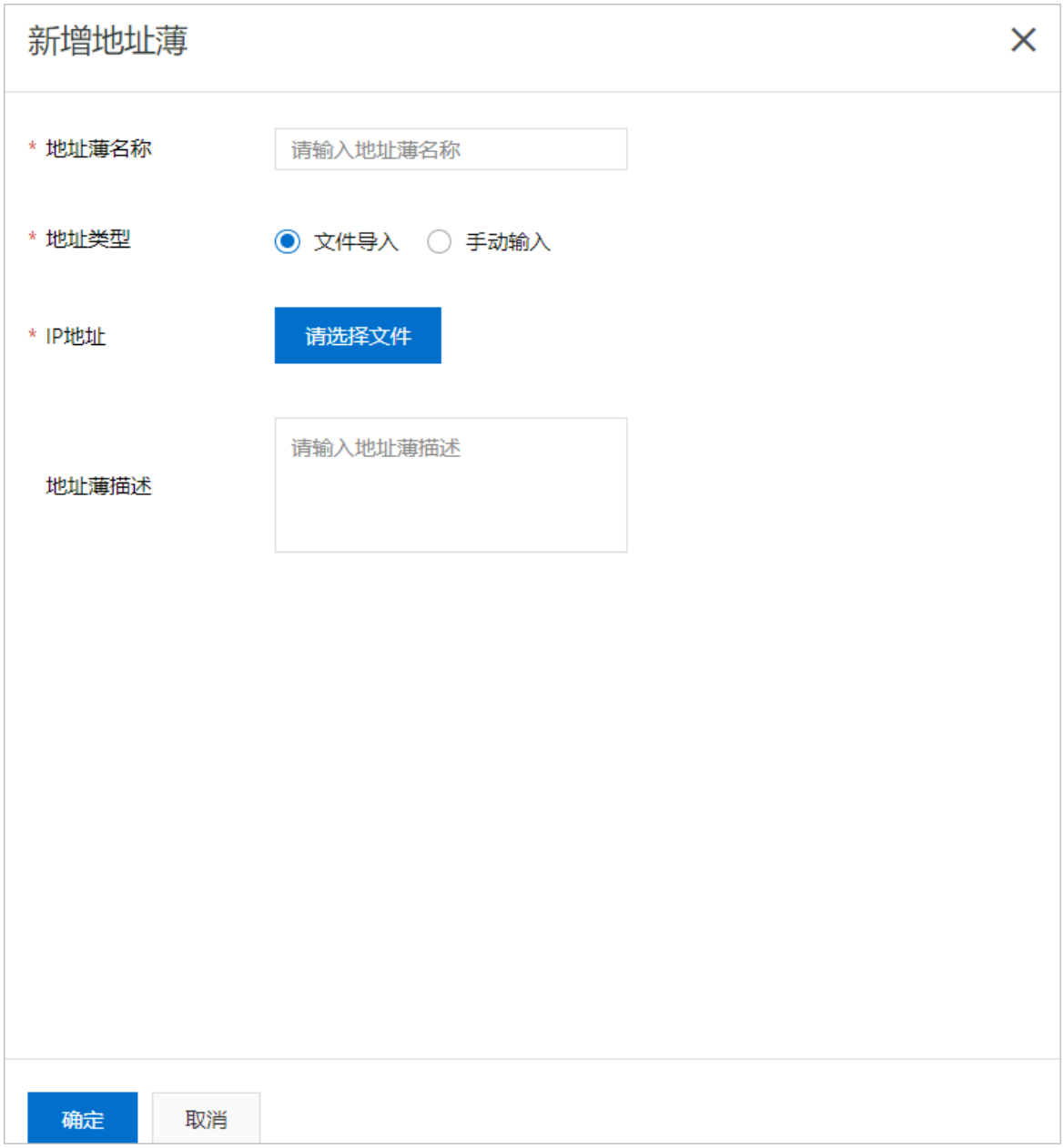
5.9.4. 管理地址簿

本文介绍了如何新增和查看地址簿。

背景信息

新增地址簿

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 单击**地址簿管理**。
5. 在**地址簿管理**页签，单击**新增IP地址簿**。
6. 在**新增IP地址簿**页面，设置参数。



参数	说明
地址簿名称	设置地址簿的名称。
地址类型	设置地址簿的地址来源类型，可选值：**文件导入**、**手动输入**。
IP地址	当**地址类型**为**文件导入**时，选择本地文件导入。当**地址类型**为**手动输入**时，需要手动输入32位IP地址。每个地址簿的IP地址，必须全部为IPv4地址或全部为IPv6地址，不能既包含IPv4地址又包含IPv6地址。
地址簿描述	设置地址簿的信息描述。

7. 单击**确定**。
   新增的IP地址簿会显示在在**地址簿管理**页签下方的IP地址簿列表。

查看地址簿

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**流量安全监控**。
3. 在左侧导航栏，单击**策略配置**。
4. 单击**地址簿管理**。
5. 在**地址簿管理**页签，查看地址簿列表。

   在地址簿列表，您还可以进行如下操作：



   - 搜索地址簿：在列表上方，您可以输入地址簿名称、地址簿描述、IP地址来进行搜索。
   - 编辑地址簿：在地址簿列表的**操作**列，单击**编辑**，您可以编辑地址簿信息。
   - 删除地址簿：在地址簿列表的**操作**列，单击**删除**，您可以删除所在行的地址簿。
   - 批量删除地址簿：您选中需要删除的地址簿前的复选框，单击**批量删除**。

6.主机安全

6.1. 主机安全总览

主机安全总览是对云主机整体的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。

在云盾安全中心的**主机安全 > 主机安全总览**中，可以查看总览、主机脆弱性趋势、资产防护、操作系统分布、最近重要脆弱性和入侵事件。



- **总览**：整体展现云主机环境各类型的安全弱点（**漏洞待处理**、**基线配置不当**）和安全事件（**入侵告警待处理**、**病毒查杀数**、**文件防篡改数**）的数量。
- **主机脆弱性趋势**：展示云主机待处理漏洞数、基线数及风险程度分布。
- **资产防护**：查看目前云主机中正在受到保护的主机数量和离线数量。
- **最近重要脆弱性和入侵事件**：展示最近重要的云主机安全弱点和安全事件，单击弱点、事件的链接可以查看具体详细情况。
- **操作系统分布**：按照操作系统类别，统计展示服务器资产。

6.2. 主机指纹

6.2.1. 管理监听端口

本文介绍如何查看服务器的对外端口监听信息，便于您快速定位可疑监听行为。

背景信息

监听端口的应用场景包括：

- 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. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**资产指纹调查**页面，单击**端口**页签，查看所有**监听端口号**、**网络协议**和服务器信息。

   您可以通过搜索端口号、服务器进程名称、服务器名称或IP，快速查找端口。

   在服务器信息列表中，查看服务器的**对应进程**、**IP**、**最新扫描时间**。

6.2.2. 管理软件版本

本文介绍如何定期查看、收集服务器的软件版本信息，便于您清点软件资产。

背景信息

软件版本的应用场景包括：

- 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.
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**软件**页签查看所有使用中的**软件资产**和使用这些软件的**服务器数**。

   您可以使用软件名、版本、软件安装目录、服务器名称或IP进行搜索。
5. 单击软件名，查看其对应资产、软件版本等信息。

   单击右上角图标，下载软件版本数据表到本地，方便后续盘点资产。

6.2.3. 管理运行进程

本文介绍定期收集服务器的进程信息，并对变动情况进行记录的方法。便于进程清点和历史进程变动查看。

背景信息

运行进程的应用场景包括：

- 清点一个进程在哪些服务器中运行。
- 清点一台服务器运行了哪些进程。

操作步骤

1.
2.
3.
4. 单击**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**、**运行用户**、**启动参数**或**服务器名称或IP**进行搜索。
5. 单击进程名，查看进程对应资产、路径、启动参数等详细信息。

6.2.4. 管理账号信息

本文介绍定期收集服务器的账号信息，并对变动情况进行记录的方法。便于账号清点和历史账号变动查看。

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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**主机指纹**页面，单击**账户**页签。
5. 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、root权限、服务器名称或IP进行搜索。
6. 单击账号名，查看对应资产、root权限、用户组等详细信息。

6.2.5. 管理计划任务

本文介绍如何收集服务器计划任务，便于您清点任务。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**主机指纹**页面，单击**计划任务**页签。
5. 查看所有任务的路径和运行这些任务的主机数。

   您可以使用任务路径、服务器名称或IP进行搜索。
6. 单击任务路径，查看对应资产、执行命令、任务周期等详细信息。

6.2.6. 设置主机指纹采集频率

通过主机指纹设置功能，选择运行进程、系统账号、开放端口、软件版本数据的采集频率。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**主机指纹**页面右上角单击**配置管理**。
5. 在相应项目的下拉菜单中，选择采集频率。
6. 单击**确定**，完成配置。

6.3. 安全预防

6.3.1. 漏洞管理

6.3.1.1. 管理Linux软件漏洞

本文介绍如何管理Linux软件漏洞。

背景信息

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.
2.
3. 在左侧导航栏，单击**漏洞管理**。
4. 在**Linux软件漏洞**页签的漏洞列表中，查看检测出的Linux漏洞。

   > **说明** 通过漏洞搜索和筛选功能，能够快速定位到具体漏洞。

5. 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。

   > **说明** 通过搜索和筛选功能，能够快速展示影响资产。

   - **基本信息**：显示该漏洞的名称、漏洞影响分值、简介和解决方案等信息。
   - **影响资产**：展示涉及该漏洞的所有服务器。
6. 根据漏洞影响情况，选择相应的处理方式。

   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：选中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。

6.3.1.2. 管理Windows系统漏洞

本文介绍如何管理Windows系统漏洞。

背景信息

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。

操作步骤

1.
2.
3. 在左侧导航栏，选择**漏洞管理**，单击**Windows系统漏洞**页签。
4. 在漏洞列表中，查看检测出的Windows系统漏洞。

   > **说明** 通过漏洞搜索和筛选功能，能够快速定位到具体漏洞。

5. 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。

   > **说明** 通过搜索和筛选功能，能够快速展示影响资产。

   - **基本信息**：显示该漏洞的名称、漏洞影响分值、简介和解决方案等信息。
   - **影响资产**：展示涉及该漏洞的所有服务器。
6. 根据漏洞影响情况，选择相应的处理方式，如漏洞操作方式所示。

   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：选中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。

6.3.1.3. 管理Web-CMS漏洞

本文介绍如何管理Web-CMS漏洞。

背景信息

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.
2.
3. 在左侧导航栏，选择**漏洞管理**，单击**Web-CMS漏洞**页签。
4. 查看所有漏洞。

   > **说明** 通过漏洞搜索和筛选功能，能够快速定位到具体漏洞。

5. 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。

   > **说明** 通过搜索和筛选功能，能够快速展示影响资产。

6. 根据漏洞影响情况，选择相应的处理方式，如漏洞操作方式所示。

   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：选中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。

6.3.1.4. 管理应急漏洞

本文介绍如何管理应急漏洞。

背景信息

云盾安全中心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. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**漏洞管理**。
4. 在**漏洞管理**页面，单击**应急漏洞**页签。
5. 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。
6. 单击漏洞名称，进入漏洞详情页，查看漏洞**详情**、**修复建议**、**受影响资产**。

   通过搜索和筛选功能，快速展示影响资产。
7. 根据漏洞影响情况，选择相应的处理方式，如漏洞操作方式所示。

   应急漏洞需要按照修复说明手动修复。

   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小时内系统会自动验证漏洞是否已修复。

   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：选中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。

6.3.1.5. 设置漏洞管理策略

漏洞管理设置允许您开启或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. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**漏洞管理**。
4. 单击右上角的**漏洞管理设置**，配置相关策略。



- 选择需要操作的漏洞类型，单击切换开关，开启或关闭该漏洞检测。
- 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。
- 选择失效漏洞自动删除周期：7天、30天、90天。

  > **说明** 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。

- 选中需要扫描的漏洞等级：
  - **高**：需尽快修复
  - **中**：可延后修复
  - **低**：暂可不修复
- 在漏洞白名单下选中相应漏洞，单击**移除**，重新启用对该漏洞的检测和告警。

6.3.2. 基线检查

6.3.2.1. 基线检查介绍

基线检查功能可自动检测服务器上的安全配置，并针对所发现的检测结果提供问题详情说明和基线加固建议。

功能描述

使用基线检查功能可自动检测服务器上的系统、账号、数据库、弱密码、合规性配置中存在的风险点，并提供加固建议。具体检测内容请参见基线检查内容。

基线检查默认每天0点到6点进行一次全面的自动检测。您可以自行添加和管理基线扫描策略，自定义需要检查的基线项目、检查周期、检测触发时间和应用该策略的服务器。具体请参见设置基线检查策略。

注意事项

以下检查项默认关闭，如果您需要检查该项目，请确认在不影响业务的情况下，在自定义基线扫描策略时选中这些检测项目。

- 部分弱密码检测项（例如，MySQL弱密码检测、PostgreSQL弱密码检测、SQLServer弱密码检测）

  > **说明** 这些检测项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成较多的登录失败记录。

- 系统等保
- CIS标准检测项

基线检查内容

基线检查项分类	检查项
高危风险利用	• 高危风险利用-CouchDB未授权访问高危风险 • 高危风险利用-Docker未授权访问高危风险 • 高危风险利用-Elasticsearch未授权访问高危风险 • 高危风险利用-Memcached未授权访问高危风险 • 高危风险利用-Apache Tomcat AJP文件包含漏洞风险 • 严重威胁利用-ZooKeeper未授权访问高危风险
	阿里云标准的安全基线检查 • 阿里云标准-Aliyun Linux 2安全基线检查 • 阿里云标准-CentOS Linux 6安全基线检查 • 阿里云标准-CentOS Linux 7安全基线检查 • 阿里云标准-Debian Linux 8安全基线检查 • 阿里云标准-Redhat Linux 6安全基线检查 • 阿里云标准-Redhat Linux 7安全基线检查 • 阿里云标准-Ubuntu安全基线检查 • 阿里云标准-Windows 2008 R2安全基线检查 • 阿里云标准-Windows 2012 R2安全基线检查 • 阿里云标准-Windows 2016/2019 R2安全基线检查

基线检查项分类	检查项
等保合规	CIS标准的安全基线检查 • CIS标准-Aliyun Linux 2安全基线检查 • CIS标准-CentOS Linux 6安全基线检查 • CIS标准-CentOS Linux 7安全基线检查 • CIS标准-Debian Linux 8安全基线检查 • CIS标准-Ubuntu 14安全基线检查 • CIS标准-Ubuntu 16/18安全基线检查 • CIS标准-Windows Server 2008 R2安全基线检查 • CIS标准-Windows Server 2012 R2安全基线检查 • CIS标准-Windows Server 2016/2019 R2安全基线检查
	等保三级合规基线检查 • 等保三级-Aliyun Linux 2合规基线检查 • 等保三级-CentOS Linux 6合规基线检查 • 等保三级-CentOS Linux 7合规基线检查 • 等保三级-Debian Linux 8合规基线检查 • 等保三级-Redhat Linux 6合规基线检查 • 等保三级-Redhat Linux 7合规基线检查 • 等保三级-SUSE 10合规基线检查 • 等保三级-SUSE 11合规基线检查 • 等保三级-SUSE 12合规基线检查 • 等保三级-Ubuntu 14合规基线检查 • 等保三级-Ubuntu 16/18合规基线检查 • 等保三级-Windows 2008 R2合规基线检查 • 等保三级-Windows 2012 R2合规基线检查 • 等保三级-Windows 2016/2019 R2合规基线检查

基线检查项分类	检查项
最佳安全实践	• 阿里云标准-Aliyun Linux 2安全基线检查 • 阿里云标准-Apache安全基线检查 • 阿里云标准-CentOS Linux 6安全基线检查 • 阿里云标准-CentOS Linux 7/8安全基线检查 • 阿里云标准-Debian Linux 8安全基线检查 • 阿里云标准-IIS 8安全基线检查 • 阿里云标准-Memcached安全基线检查 • 阿里云标准-MongoDB 3.x版本安全基线检查 • 阿里云标准-Mysql安全基线检查 • 阿里云标准-Nginx安全基线检查 • 阿里云标准-Redhat Linux 6安全基线检查 • 阿里云标准-Redhat Linux 7安全基线检查 • 阿里云标准-Redis安全基线检查 • 阿里云标准-Ubuntu安全基线检查 • 阿里云标准-Windows 2008 R2安全基线检查 • 阿里云标准-Windows 2012 R2安全基线检查 • 阿里云标准-Windows 2016/2019 R2安全基线检查 • 阿里云标准-Apache Tomcat 安全基线检查
弱口令	• 弱口令-MongoDB登录弱口令检测(支持2.x版本) • 弱口令-FTP登录弱口令检查 • 弱口令-Linux系统登录弱口令检查 • 弱口令-MongoDB登录弱口令检测 • 弱口令-SQL Server数据库登录弱口令检查 • 弱口令-Mysql数据库登录弱口令检查 • 弱口令-Mysql数据库登录弱口令检查(Windows版) • 弱口令-PostgreSQL数据库登录弱口令检查 • 弱口令-Redis数据库登录弱口令检查 • 弱口令-rsync服务登录弱口令检查 • 弱口令-svn服务登录弱口令检查

6.3.2.2. 设置基线检查策略

本文介绍如何如何新增、编辑、删除基线检查策略，并设置基线检查等级的范围。

背景信息

默认情况下，基线检查会使用**默认策略**检测资产的基线安全情况。您可以根据实际业务情况（例如需要满足等保二级），自定义基线检查策略。

操作步骤

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**基线检查**。
4. 单击控制台界面右上角**策略管理**，在**策略管理**页面，新增、修改或删除自定义基线检查策略，或修改默认策略。
   - 单击策略列表右上角的**添加策略**，自定义基线检查策略后单击**确定**。

配置项	说明
策略名称	输入用于识别该策略的名称。
检测周期	选择检测周期（每隔1天、3天、7天、30天检测一次）和检测触发时间（00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00）。
基线名称	选中需要检测的基线项目，在数据库、系统、弱密码检测、中间件下选中具体需要检测的内容。
生效服务器	选中需要应用该策略的分组资产。 **说明** 新购买的服务器默认归属在**分组资产 > 未分组**中，如需对新购资产自动应用该策略，请选中**未分组**。

   - 单击策略名称后的**编辑**或**删除**，对已有策略进行修改或删除。

     说明 策略删除后不可恢复。

   - 单击策略模板列表中**默认策略**右侧**操作**栏的**编辑**，调整应用默认策略的资产分组。

     说明 默认策略不支持删除，检测项不支持更改，仅支持修改应用默认策略的资产分组。

   - 在**策略管理**页面下方，您可以设置基线检查的等级范围（高、中、低）。
5. 单击**确定**。

6.3.2.3. 查看和处理基线检查结果

云盾控制台提供了检查后的基线详情说明、基线加固建议和风险处理功能。本文介绍如何在云盾控制台查看和处理基线项目的检查结果，具体包括查看基线项目影响的资产、基线项目详情等信息，以及如何对风险项进行处理。

查看检测结果总览数据

1.
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**基线检查**。
4. 在**基线检查**页面上方，查看云盾控制台根据不同基线检查策略，在您资产中检测到的基线检查结果汇总数据。



在**基线检查策略**下拉框中选择目标基线检查策略，查看以下信息。

- **服务器**：执行基线检查的服务器数量，即配置基线检查策略时，选中的分组服务器中服务器的总台数。
- **检查项**：配置基线检查策略时，选中的**基线名称**的数量。
- **通过率**：最近一次执行基线检查的基线合格率。

  通过率字体为绿色时，代表扫描的资产中基线配置合格率较高；字体为红色时，说明检查的资产中不合格的基线配置较多，可能存在安全隐患，建议前往基线检查详情页面查看并修复。

查看基线检查项目列表

1.
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**基线检查**。
4. 在**基线检查策略**下拉框中选择**全部策略**。
   基线检查页面会展示所有基线检查项目的列表，包括**基线名称**、**基线检查项**、**风险项/影响服务器数**、**基线分类**及**最新检查时间**。

> **说明** 您也可在**基线检查策略**下拉框中选择某个基线检查策略，查看该策略对应的基线检查项目列表。

查看基线项目详情

1.
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**基线检查**。
4. 在基线检查列表的**基线名称**列中，单击待查看的基线项目，展开该基线项目的详情页面。
5. 在基线详情页面对检测出的风险项进行处理。
   - 单击待查看资产右侧**操作**列下的**查看**，进入**风险项**页面，查看风险检查项详情。
   -

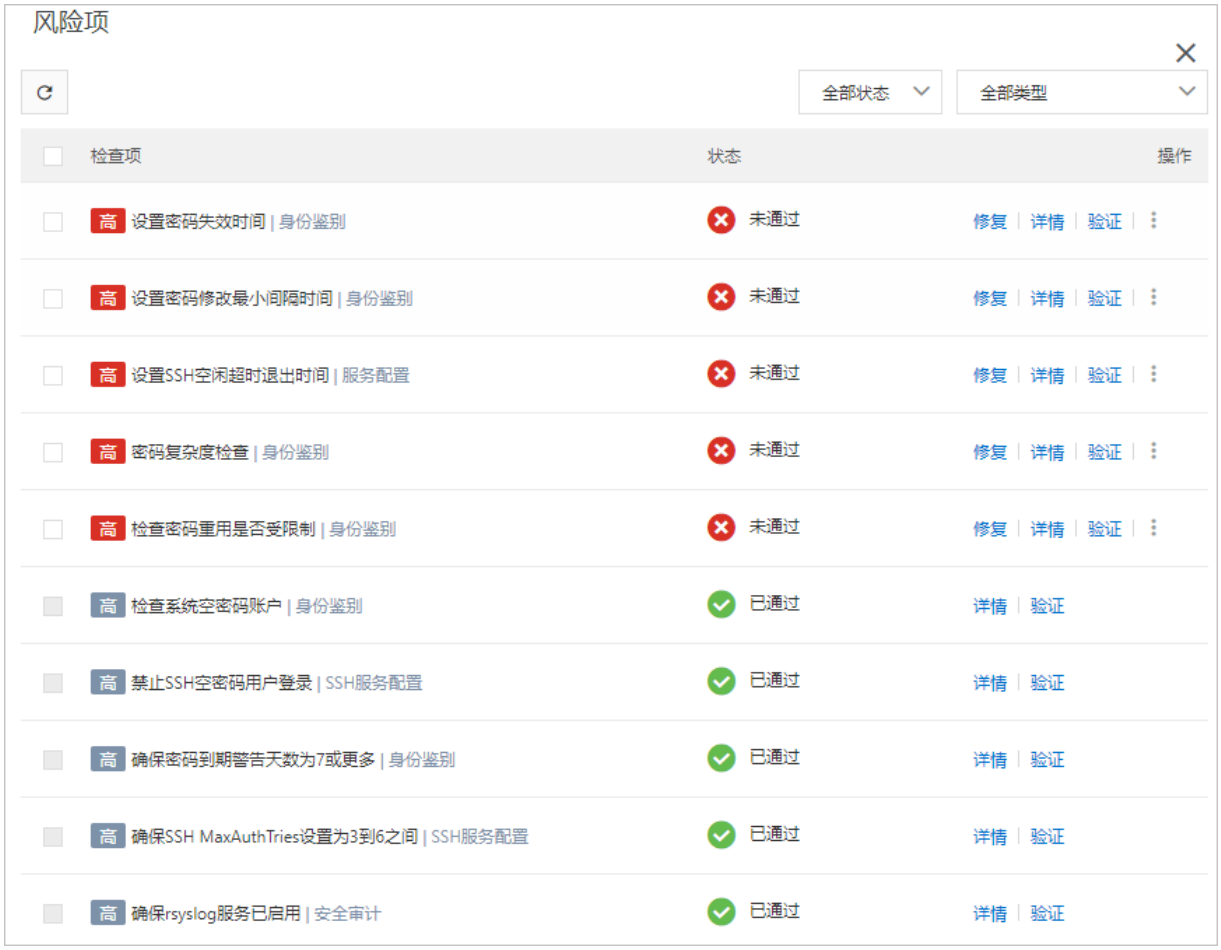
查看风险项详情

1. 在基线项目详情页面，单击待查看风险项资产右侧**操作**列下的**查看**，展开该资产的风险项页面。
   您可查看到该资产详细的基线配置检查项及检查项对应的检查结果（**已通过**/**未通过**）。
2.

> **说明** 建议您根据加固建议及时修复**未通过**的基线检查项目，尤其是高危险等级的风险项。

处理风险检查项

在风险项列表中，根据需要对风险检查项进行相应的处理。



- **加入白名单**

  如果您不希望收到指定的基线检查项的告警，可对指定检查项执行**加白名单**操作。加入白名单后，该基线检查项将不再触发告警。

  > 说明 选中多个检查项后，单击左下角的**加白名单**，可批量将多个检查项加入白名单。

- **修复**

  仅支持阿里云标准基线检查项的批量修复，修复时可选择多台具有相同基线风险的服务器。

  > 注意 基线修复存在一定的风险，请在修复前请确认已做好备份。

- **取消已忽略的基线检查配置项告警**

  如果需要云盾控制台对已忽略的基线检查配置项再次触发告警，可对已忽略的检查项执行**取消加白**。支持单个或批量取消忽略的操作。取消加白后，该基线检查配置项会再次触发告警。

- **验证已修复的基线检查配置项**

  如果未进行手动验证，将会根据在扫描策略中设置的检测周期执行自动验证。

6.4. 入侵防护

6.4.1. 入侵事件

6.4.1.1. 入侵事件类型概述

主机安全支持敏感文件篡改、进程异常行为、网站后门、异常登录、恶意进程等安全告警类型，通过全面的安全告警类型帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

云盾安全中心可对您已开启的告警防御能力提供总览数据，帮助您快速了解已开启和未开启的防御项目。您可在**入侵事件**页面，查看安全告警的统计和防御项目的信息。

安全告警类型列表

防御项目包含的内容如下所示：

告警名称	告警说明
威胁情报	基于专有云云盾威胁情报，安骑士能够有效识别资产中的潜在威胁。威胁情报可以对威胁信息的相关内容进行关联、分析和处理，发现威胁后及时告警，从而提升威胁检查效率和响应速度。 • 恶意域名 • 恶意IP • 暗网通信IP • 中控通信IP • 矿池通信IP • 恶意URL • 恶意下载源
异常登录	检测服务器上的异常登录行为。通过设置合法登录IP、时间及账号，对于例外的登录行为进行告警。支持手动添加和自动更新常用登录地，对指定资产的异地登录行为进行告警。 可检测以下子项： • ECS非合法IP登录 • ECS在非常用地登录 • ECS登录后执行异常指令序列（SSH） • ECS被暴力破解成功（SSH）
网站后门	使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能： • Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。 • 支持针对网站后门检测的资产范围配置。 • 对发现的木马文件支持隔离、恢复和忽略。
精准防御	**病毒查杀**功能提供了精准防御能力，可对主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等类型进行防御。

告警名称	告警说明
异常账号	检测非合法的登录账号。
云产品威胁检测	检测其他云产品中是否存在威胁。
持久化后门	检测服务器上存在的可疑计划任务，对攻击者持久入侵用户服务器的威胁行为进行告警。
异常网络连接	检测网络显示断开或不正常的网络连接状态。
进程异常行为	检测资产中是否存在超出正常执行流程的行为。
恶意进程（云查杀）	采用云+端的查杀机制，对服务器进行实时检测，并对检测到的病毒文件提供实时告警。您可通过控制台对病毒程序进行处理。 可检测以下子项： • 访问恶意IP • 挖矿程序 • 自变异木马 • 恶意程序 • 木马程序
敏感文件篡改	检测是否存在对服务器中的敏感文件进行恶意修改，包含Linux共享库文件预加载配置文件的可疑篡改等行为。
其他	检测DDoS流量攻击等网络入侵行为。
Web应用威胁检测	检测通过Web应用入侵服务器的行为。
应用入侵事件	检测通过系统的应用组件入侵服务器的行为。

6.4.1.2. 查看和处理入侵事件

您可以在入侵事件页面查看和处理已检测出的告警事件。

背景信息

云盾检测出安全告警事件后，会在控制台**入侵事件**页面展示相关告警信息。如果告警事件未被处理，会展示在**入侵事件**页面的**待处理告警**列表中。告警事件处理完成后，将从**待处理告警**状态转化为**已处理**。

> **说明** 在**入侵事件**页面为您一直保留**待处理告警**和**已处理告警**记录。默认展示**待处理告警**记录。

查看告警事件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在入侵事件列表中，查看或搜索所有检测到的入侵和威胁告警及其详细信息。

处理告警事件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在**入侵事件**页面，定位到目标告警事件，单击**操作**栏的**处理**，对不同告警事件执行相应的处理后单击**立即处理**。

   > **说明** 如果告警事件包含多个关联异常，单击**处理**，会打开该告警事件的详情页面，您可对不同的异常事件分别进行处理。

   - **忽略**：忽略本次告警，该告警状态将变为**已处理**，后续不会再对该事件进行告警。
   - **加白名单**：如果告警为误报，您可以将本次告警加入白名单。告警加入白名单后该告警状态将变为**已处理**，后续安骑士不会再对该事件进行告警。您可以在**已处理**列表中定位到该事件对其进行**取消白名单**的操作。

     > **说明** 告警误报是指系统对正常程序进行告警。常见的告警误报有**对外异常TCP发包可疑进程**，提示您服务器上有进程在对其他设备发起了疑似扫描行为。

   - **同时处理相同告警**：对多个告警事件进行批量处理。批量处理告警事件前，请详细了解告警事件的信息。
5. （可选）如果您已确认一个或多个告警事件需要忽略或为误报，可在**入侵事件**页面，选中一个或多个告警事件，直接进行**忽略本次**或**加白名单**处理。

导出告警事件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 单击**入侵事件**页面危险等级栏  图标，导出报表。

   报表导出完成后，安全告警页面右上角会提示**导出完成**。
5. 在**安全告警处理**页面右上角**导出完成**对话框中，单击**下载**。
   安全告警事件文件会下载到本地。

6.4.1.3. 查看告警自动化关联分析

安骑士支持告警自动化关联分析。您可在安全告警列表页面单击单个告警事件名称进入告警自动关联分析页面，查看和处理告警事件所有关联的异常情况并进行攻击自动溯源，帮助您对告警事件进行全方位分析和便捷处理。

背景信息

- 告警自动关联分析功能可对相关的异常事件进行实时自动化关联，挖掘出潜藏的入侵威胁。
- 告警自动化关联以告警发生的时间顺序聚合成关联的告警，帮助您更便捷地分析和处理告警事件，提升您系统的应急响应机制。

- 告警自动化关联分析聚合后的告警以 图标标识。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在入侵事件列表中，单击目标**告警名称**打开告警事件详情面板。
5. 在告警事件详情面板，查看告警事件的详细信息、关联的异常事件和对告警的异常事件进行处理。
   - 查看告警详细信息

     您可查看受该告警事件影响的资产信息、告警首次发生或最新发生时间、关联异常事件的详情。
   - 查看受影响资产

     鼠标悬停在**受影响资产**名称上，会弹出对应资产的详情页面，方便您集中查看该资产的全部告警信息、漏洞信息、基线检查漏洞和资产指纹等信息。
   - 查看和处理**关联异常**

     您可在**关联异常**区域查看该告警事件关联的所有异常情况的详细信息和建议方案。
     - 单击各关联异常区域右侧的**备注**，可为该关联异常事件添加备注信息。
     - 单击备注信息右侧的 × 图标，即可删除备注信息。

6.4.1.4. 文件隔离箱

安骑士可对检测到的威胁文件进行隔离处理，被成功隔离的文件会添加到安全告警处理页面的文件隔离箱中。被成功隔离的文件可在30天内进行一键恢复，且隔离30天后系统将自动清除被隔离文件。本文介绍了如何查看隔离文件和解除文件隔离。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在**入侵事件**页面单击右上角**文件隔离箱**。

   您可在**文件隔离箱**进行以下操作：
   - 在文件隔离箱列表中可以查看被隔离的文件主机地址、文件路径、状态和修改时间等信息。
   - 单击文件隔离箱页面右侧**操作**栏的**恢复**，可以将指定的被隔离文件从文件隔离箱中移除。恢复的文件将重新回到安全告警列表中。

6.4.1.5. 安全告警设置

安骑士的安全告警设置支持手动维护常用登录地和Web目录，并支持高级登录报警功能。

背景信息

安骑士提供高级登录报警功能，支持配置更精细的异常登录检测，例如设置合法登录的IP、时间、账号。

操作步骤

1.
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 单击页面右上角**安全告警设置**。

   选择相应的功能页签，完成以下配置：

   - **添加常用登录地**

     a. 单击**常用登录地**右侧的**管理**按钮。

     b. 选中要添加的常用登录地点，然后选择添加应用的服务器。

     c. 单击**确定**，完成添加。

     安骑士支持**编辑**和**删除**已成功添加的常用登录地。

     - 单击目标常用登录地右侧的**编辑**，修改该登录地的生效服务器。
     - 单击目标常用登录地右侧的**删除**，删除该常用登录地配置。

   - **配置高级登录报警**

     > **说明** 配置高级登录告警，可进一步指定常用的登录IP、时间段和账号。配置完成后，安骑士会对指定外的登录情形进行告警。以下功能的操作类似**常用登录地**配置，可参考上文进行**添加**、**编辑**、**删除**。

     - 单击**常用登录IP**右侧的切换开关，打开或关闭登录IP检查，开启后通过非指定IP登录会触发报警。
     - 单击**常用登录时间**右侧的切换开关，打开或关闭登录时间检查，开启后在非指定时间登录会触发报警。
     - 单击**常用账号**右侧的切换开关，打开或关闭登录账号检查，开启后使用非指定账号登录会触发报警。

   - **自定义Web目录**

     安骑士会自动检测您服务器资产中的Web目录，并进行动态检测和静态扫描；您也可以手动添加服务器中的其它Web目录进行检测扫描。

     a. 单击**Web目录定义**右侧的**管理**。

     b. 输入一个合法的Web路径，然后选中生效服务器，该路径将被添加到扫描路径的服务器。

     > **说明** 出于性能效率考虑，不支持直接添加root目录作为Web目录。

     c. 单击**确定**，完成添加。

6.4.1.6. 病毒云查杀

云盾安骑士病毒查杀（以下简称“云查杀”）集成了中国及中国以外地域多个主流的病毒查杀引擎，并利用阿里云海量威胁情报数据和自主研发的基于机器学习、深度学习异常检测模型，为用户提供全面和实时的病毒检测和防护服务。

目前云查杀每天检测数亿文件，实时服务百万云上服务器。

云查杀检测能力

安骑士采用云+端的查杀机制，客户端负责采集进程信息，上报到云端控制中心进行病毒样本检测。若判断为恶意进程，支持用户进行停止进程、隔离文件等处理。

云查杀具有以下检测能力：

- **深度学习检测引擎（自主研发）**：云盾深度学习检测引擎，使用深度学习技术，基于海量攻防样本，专门打造的一款适用于云环境的恶意文件检测引擎，智能识别未知威胁，是传统病毒查杀引擎的有力支撑。
- **云沙箱（自主研发）**：真实还原云上环境，监控恶意样本攻击行为，结合大数据分析、机器学习建模等技术，自动化检测和发现未知威胁，提供有效的动态分析检测能力。
- **集成中国及中国以外地域主流病毒查杀引擎**：云查杀集成中国及中国以外地域多款优秀的杀毒引擎，可对病毒库进行实时更新。
- **威胁情报检测**：基于云盾威胁情报数据，配合服务器异常行为检测模型，实现多维度检测异常进程和恶意行为。

云查杀覆盖的病毒类型

云查杀是阿里云安全技术与攻防专家经验融合的最佳实践，从数据的采集、脱敏、识别、分析、隔离到恢复，已形成安全闭环，同时支持用户在云盾控制台中对云查杀结果进行隔离和恢复处理。

云查杀覆盖以下病毒类型：

病毒类型	病毒描述
挖矿程序	非法占用服务器资源进行虚拟货币挖掘的程序。
蠕虫病毒	利用网络进行复制和传播的恶意程序，能够在短时间内大范围传播。
勒索病毒	利用各种加密算法对文件进行加密，感染此病毒一般无法解密，如WannaCry等。
木马程序	特洛伊木马，可受外部用户控制以窃取服务器信息或者控制权、盗用用户信息等的程序，可能会占用系统资源。
DDoS木马	用于控制肉鸡对目标发动攻击的程序，会占用本机带宽攻击其他服务器，影响用户业务的正常运行。
后门程序	黑客入侵系统后留下的恶意程序，通过该程序可以随时获得服务器的控制权或进行恶意攻击。
病毒型感染	运行后感染其他正常文件，将可能携带有感染能力的恶意代码植入正常程序，严重时可能导致整个系统感染。
恶意程序	其他威胁系统和数据安全的程序，例如黑客程序等。

云查杀的优势

- **自主可控**：基于自主研发的深度学习、机器学习能力及大数据攻防经验，并结合多引擎检测能力，为您提供全面、实时的病毒检测服务。
- **轻量**：Agent客户端仅占用1%的CPU、50 MB内存，不影响业务的运行。
- **实时**：获取进程启动日志，实时监控病毒程序的启动。
- **统一管理**：云安全中心控制台支持对所有服务器进行统一管理，实时查看所有服务器的安全状态。

安全威胁防御限制说明

云盾控制台支持安全告警实时检测与处理、漏洞检测与一键修复、攻击分析、云平台安全配置检查等功能，结合告警关联分析和攻击自动化溯源，帮助您全面加固系统和资产的安全防线。在云盾安骑士提供的防御能力以外，建议您定期更新服务器安全系统补丁、配合使用云防火墙、Web应用防火墙等产品缩小网络安全威胁的攻击范围，实时预防，不让黑客有任何可乘之机。

> **说明** 由于网络攻击手段、病毒样本在不断的演变，实际的业务环境也有不同差异，因此无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查、云平台配置检查等安全能力，提升整体安全防线，预防黑客入侵、盗取或破坏业务数据。

6.4.2. 网页防篡改

6.4.2.1. 概述

防篡改可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

背景信息

网络攻击者通常会利用被攻击网站中存在的漏洞，通过在网页中植入非法暗链对网页内容进行篡改等方式，进行非法牟利或者恶意商业攻击等活动。网页被恶意篡改会影响用户正常访问网页内容，还可能会导致严重的经济损失、品牌损失甚至是政治风险。

网页防篡改支持将Linux和Windows服务器进程加入白名单，可实现网站防护文件实时更新。

防护原理

云盾Agent通过自动化采集获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对异常文件的进程进行阻断。

您可以在云盾主机安全防篡改页面的告警列表中，查看被云盾检测出的异常文件变动告警、异常进程和该进程尝试写文件的次数。如果您确定该异常文件相关的进程是正常的业务结果，可以将该进程添加到白名单中。防篡改功能不再对加入到白名单中的进程进行拦截。对于新闻、教育类网站需要频繁修改网站内容的场景，可有效避免需要频繁开启和关闭防篡改功能的问题。

防篡改支持的系统内核版本

OS	支持的OS版本	支持的内核（Kernel）版本
Windows	Windows Server 2008及以上版本	所有版本
CentOS	6.5、6.6、6.7、6.8、6.9、6.10、7.0、7.1、7.2、7.3、7.4、7.5、7.6	• 2.6.32-x • 3.10.0-x

OS	支持的OS版本	支持的内核（Kernel）版本
Ubuntu	14、16、18	• 3.13.0-32-generic • 3.13.0-86-generic • 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-151-generic • 4.4.0-117-generic • 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic

> **说明**
>
> - 目前，防篡改支持的服务器kernel版本有限，不在支持范围内的服务器将无法使用防篡改进程白名单功能。请确认您的服务器kernel版本是否在上述支持列表覆盖范围内。如果不在支持范围内，需要手动升级kernel到支持列表里的版本，才能使用进程加白名单的功能。
> - 升级服务器kernel前请使用快照备份您的资产数据。

6.4.2.2. 创建网页防篡改保护

主机安全支持对主机开启网页防篡改防护，全面保护您网站的安全。

限制条件

- 每台服务器最多可添加10个防护目录。
- Windows系统单个防护目录大小不超过20 GB；单个防护目录下的文件夹不超过2000个；防护目录文件夹层级不超过20个；单文件大小不超过3 MB。
- Linux系统单个防护目录大小不超过20 GB；单个防护目录下的文件夹不超过3000个；防护目录文件夹层级不超过20个；单文件大小不超过3 MB。
- 建议您开启防护前检查文件夹目录层级、文件夹个数和防护目录大小是否超过限制。
- 建议您排除*LOG*、*PNG*、*JPG*、*MP4*、*AVI*、*MP3*等无需进行防护的文件类型，多个文件类型之间用半角分号（;）隔开。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**防篡改**。
4. 在**防篡改**页面单击**创建网页防篡改**。
5. 在**创建网页防篡改**对话框中选中目标服务器。



6. 单击**下一步**，进入**添加防护目录**页签。
7. 在**添加防护目录**页签中，完成以下配置。



选择防护模式。可选**白名单模式**或**黑名单模式**。白名单模式下，会对添加的防护目录和文件类型进行保护；黑名单模式下，会防护目录下所有未排除的子目录、文件类型和指定文件。默认开启白名单模式。

- 白名单模式配置：

配置项	描述

配置项	描述
防护目录	手动输入该服务器下需要开启防篡改保护的目录地址。 **说明** Linux服务器和Windows服务器防护目录地址的格式可能会有区别，请根据页面提示输入正确的格式。
防护文件类型	单击下拉列表，选择该目录中需要防护的文件类型，例如：*JS*、*HTML*、*XML*、*JPG*等。
本地备份目录	展示防护目录的默认备份存储路径。 云盾安全中心为您指定的默认备份目录为*/usr/local/aegis/bak*（Linux服务器）和*C:\Program Files (x86)\Alibaba\Aegis\bak*（Windows服务器），您可手动修改默认的备份路径。

- 黑名单防护模式：

配置项	描述
防护目录	手动输入该服务器下需要开启防篡改保护的目录地址。
排除子目录	手动输入无需开启网页防篡改的子目录地址。 单击**添加子目录**，支持添加多个子目录。 添加排除子目录后，云盾安全中心将不会对该子目录中的文件进行防护。
排除文件类型	选择无需进行网页防篡改检测的文件格式。 可选值包含**log**、**txt**、**ldb**。 选择排除文件类型后，云盾安全中心将不会对该防护目录下该类型的文件进行防护。
排除指定文件	手动输入无需开启网页防篡改的文件目录地址。 单击**添加文件**，支持添加多个文件。 输入指定文件后，云盾安全中心将不会对该指定文件进行防护。
本地备份目录	展示防护目录的默认备份存储路径。 云盾安全中心为您指定的默认备份目录为*/usr/local/aegis/bak*（Linux服务器）和*C:\Program Files (x86)\Alibaba\Aegis\bak*（Windows服务器），您可手动修改默认的备份路径。

8. 单击**开启防护**，完成添加服务器和目录的操作。
   添加服务器完成后，该服务器将显示在**网页防篡改**页面的防护服务器列表中。

   说明 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**页面**开启**目标服务器的防护状态。

9. 在**防篡改**页面，单击**防护管理**页签，打开目标服务器**防护状态**开关，为该服务器开启防护服务。



> **说明** 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**列表中开启目标服务器的防护状态。

启动成功后服务状态将会显示为**正在运行**。

> **说明** 当防护服务状态为**异常**时，在目标服务器服务状态栏单击**异常**，显示异常状态的详细原因并单击**重试**。

后续操作

为服务器开启网页防篡改保护后，您可在**安全告警处理**页面，筛选网页防篡改类型，查看云盾安全中心为您检测到的网页篡改事件和告警信息。

> **说明**
>
> 配置完成防护目录后网页防篡改未立即生效，并且此时仍然可以对该防护目录写入文件。这种情况下，您需在**防护管理**列表中对该目录所在的服务器关闭**防护状态**开关，然后重新打开**防护状态**开关。

防护异常状态处理

服务状态	说明	建议
启动中	网页防篡改防护状态正在开启。	首次开启防护时，目标主机的服务状态将会显示为**启动中**。请耐心等待数秒。
正在运行	防护状态已成功开启，并正常运行中。	无。
异常	防护开启异常。	在目标主机服务状态栏单击**异常**，查看发生异常的原因并重试。
未启动	防护状态为未开启。	需将防护状态设置为**开**。

6.4.2.3. 查看防护状态

本文介绍了如何查看您资产的网页防篡改防护状态。

背景信息

网页防篡改功能可实时监控网站目录文件的变化并对异常的文件变动事件进行拦截。您可以在云盾控制台**主机安全 > 入侵防护 > 防篡改**页面查看到安骑士为您检测到的网页防篡改防护状态和信息，包括：

- 网页防篡改统计数据总览



  您可以在统计数据总览模块中查看当天以及最近15天内发生变动的文件总数、已被防护的服务器数量和目录数量。

- 防篡改防护文件类型分布数据

  防护文件类型包括TXT、PNG、MSI、ZIP等文件类型。您也可以手动添加需要防护的其他文件类型。

  > **说明** 目前防护文件类型不受限制，所有文件类型都支持网页防篡改防护。

- 文件变动数Top 5

  该模块展示了最近15天内检测到的变动次数排名前5的文件名称和文件所在路径。

- 网页防篡改告警详情列表。



  该列表展示了网页防篡改功能为您资产拦截到的所有异常文件变动及其详细信息，包括告警等级、告警名称、受影响资产、异常变动文件的路径、防御状态等信息。

  > **说明**
  > - 如果告警尝试次数（进程写文件次数）超过100次，建议您及时关注并处理该告警。
  > - 目前告警等级只有**中危**等级。
  > - 防御状态只有**已防御**一种状态，表示网页防篡改功能在检测到异常文件变动事件时，已及时为您拦截执行该异常变动的进程。

6.4.3. 病毒查杀

安骑士的病毒查杀设置功能提供自定义配置病毒查杀和网站后门查杀管理的服务。

病毒查杀

病毒查杀能够帮助您自动隔离常见网络病毒，包括主流木马病毒、勒索软件、挖矿病毒、DDoS木马等。所有支持自动隔离的病毒都经过了云盾安全专家的测试和验证，确保零误杀。

未开启自动隔离时，云盾安骑士以安全告警的形式向您展示在服务器上检测出的病毒，您需要在控制台手动处理。建议您开启病毒自动隔离，加固主机安全防线。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**病毒防御**。
4. 在**病毒查杀**页签下，单击**开始病毒扫描**。
5. 在弹出的对话框中，选中您要扫描的资产。
6. 单击**开始扫描**。
7. 在**病毒防御**页面，单击**实时防护**页签开关，开启病毒查拦截功能。

   开启病毒拦截后，安骑士将对检测出的主流病毒类型进行自动隔离，您可在安全告警处理页面**精准防御**类型告警列表中，查看被病毒查杀功能自动隔离掉的病毒。

网站后门查杀

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**病毒防御**。
4. 配置对网站服务器网页目录进行检测和识别网站后门的检测范围。
   i. 在**网站后门查杀**区域，单击**管理**。
   ii. 选择哪些服务器需要进行网站后门查杀。
   iii. 单击**确定**，完成配置。

6.5. 日志检索

6.5.1. 日志检索介绍

云主机安全提供主机日志检索功能，将散落在专有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

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。

6.5.2. 查询日志

本文介绍如何搜索和查看主机日志。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**日志检索**。
4. 设置搜索条件。

搜索项	说明
请选择日志源	支持的日志源，具体内容请参见日志源。
请选择字段	各日志源支持的字段，具体内容请参见日志源。
关键字	需要搜索的字段具体关键字。
语法逻辑	等于。
+	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）。

5. 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。

6.5.3. 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。

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

登录流水查询支持下表描述的字段。

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

暴力破解

暴力破解查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	攻击来源IP

字段	数据类型	说明
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

进程启动日志

进程启动日志查询支持下表描述的字段。

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

端口监听快照

端口监听快照查询支持下表描述的字段。

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

字段	数据类型	说明
proc_path	string	进程路径
pid	string	进程ID
proc_name	string	进程名
proto	string	协议

账号快照

账号快照查询支持下表描述的字段。

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	账号超期时间
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

进程快照

进程快照查询支持下表描述的字段。

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1 MB不计算

网络连接日志

网络连接日志查询支持下表描述的字段。

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

6.5.4. 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。

语法逻辑说明

逻辑名称	描述
and	双目运算符。 形式为 `query 1 and query 2` ，搜索结果展示 `query 1` 和 `query 2` 查询结果的交集。 **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 `query 1 or query 2` ，搜索结果展示 `query 1` 和 `query 2` 查询结果的并集。
not	双目运算符。 形式为 `query 1 not query 2` ，搜索结果展示符合 `query 1` 并且不符合 `query 2` 的结果，相当于 `query 1 - query 2` 。 **说明** 如果只有 `not query 1` ，那么表示从全部日志中选取不包含 `query 1` 的结果。

6.6. 设置

6.6.1. 安装客户端

本文介绍了如何通过安骑士设置选项，完成安装Agent插件的方法。

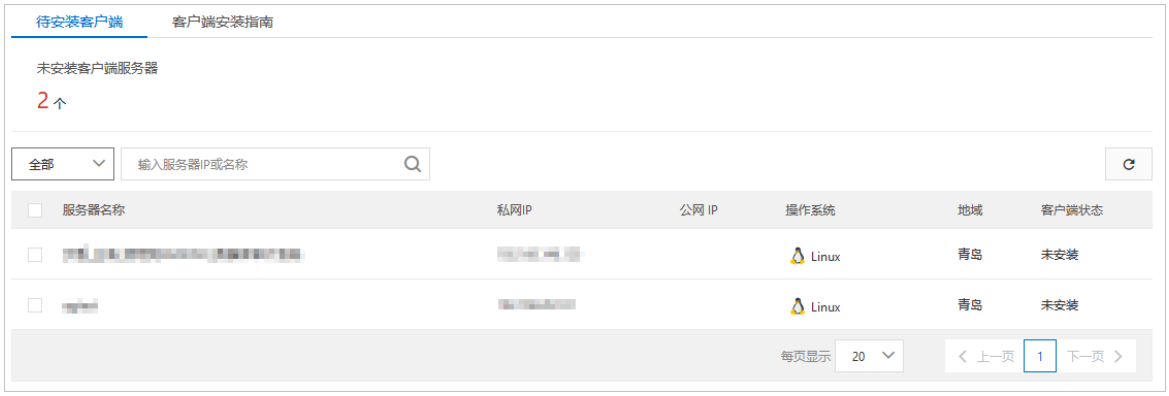
背景信息

安骑士Agent是安骑士提供的本地安全插件，您必须在服务器操作系统上安装安骑士Agent，才能使用安骑士提供的安全防护服务。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**客户端安装**。
4. （可选）单击**待安装客户端**页签，查看未安装客户端的服务器数量及其列表信息。

   您可以通过选择服务器操作系统类型、输入服务器IP或名称进行搜索，从而快速定位到目标服务器。



5. 单击**客户端安装指南**页签。
6. 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**
     a. 在左侧区域，单击**点击下载**，下载安装文件到本地计算机。
     b. 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。
     c. 在Windows服务器上，以管理员权限运行安装文件，完成安装。

     > **说明** 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**
     a. 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。
     b. 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**。
     c. 以管理员身份登录您的Linux服务器。
     d. 在Linux服务器上执行安装命令，下载和安装安骑士Agent插件。

6.6.2. 管理防护模式

本文介绍了如何管理云主机的防护模式，使服务器更高效、更安全。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**防护模式管理**。
4. 在**防护优先模式**页面，单击**管理**。

   设置服务器的防护模式。
   - **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。


防护模式管理
业务优先模式 | 3
请输入服务器IP
192.
172.
172.
3 项
防护优先模式 | 1
请输入服务器IP
43.17.
1 项
确定

5. 单击**确定**，完成配置。

7.物理机主机安全

7.1. 创建和授权账号

物理机主机安全用于保障平台侧物理机的主机安全，需要专门用于平台侧的安全管理账号。本文介绍如何创建和授权该安全管理账号。

操作步骤

1. 使用系统管理员登录Apsara Uni-manager运营控制台。

   具体操作，请参见*Apsara Uni-manager运营控制台 用户指南*的**登录Apsara Uni-manager运营控制台**章节。

2. 创建专门用于管理物理机主机安全的组织并获取组织的PrimaryKey。

   > **注意** 请确保该组织仅用于管理物理机主机安全等平台安全产品，请勿添加任何ECS实例到该组织。

   i. 创建组织。

      具体操作，请参见*Apsara Uni-manager运营控制台 用户指南*的**企业中心 > 组织管理 > 创建组织**。

   ii. 获取组织的**PrimaryKey**。

      具体操作，请参见*Apsara Uni-manager运营控制台 用户指南*的**企业中心 > 组织管理 > 获取组织AccessKey**。

3. 创建专门用于管理物理机主机安全的账号。

   具体操作，请参见 *Apsara Uni-manager运营控制台 用户指南*的**企业中心 > 用户管理 > 系统用户管理 > 创建用户**。

   > **说明** 创建账号时，**组织**和**角色**要求如下：
   > - 在**组织**中选择上个步骤中新创建的组织。
   > - 在**角色**中选择**平台安全配置管理员**和**安全系统配置管理员**。

4. 使用新创建的账号登录云盾安全中心。

   具体操作，请参见登录云盾安全中心。

5. 在物理机主机防护配置中添加组织的**PrimaryKey**。

   i. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。

   ii. 在左侧导航栏，单击**全局设置**。

   iii. 在**全局设置**页面，单击**物理主机防护配置**页签。

   iv. 单击**添加账号**。

v. 在**添加物理机安骑士账号**对话框中，填写**用户名**和**所属部门Primary Key**信息。



- **用户名**为上面步骤中创建的账号。
- **所属部门Primary Key**为上面步骤中获取的组织PrimaryKey。

vi. 单击**确定**，完成配置。

执行结果

设置完成后，您可以使用本章节创建的账号维护平台的物理机安全。

7.2. 主机列表

7.2.1. 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. 请使用创建和授权的账号，登录云盾安全中心。

   创建和授权账号的具体操作，请参见创建和授权账号章节。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机列表**。
4. 在左侧导航栏中，选择**物理机主机安全 > 主机列表**。
5. 在左侧分组区域，管理分组。



- 新建子分组。

  单击**所有资源**或者子分组右侧的＋，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。

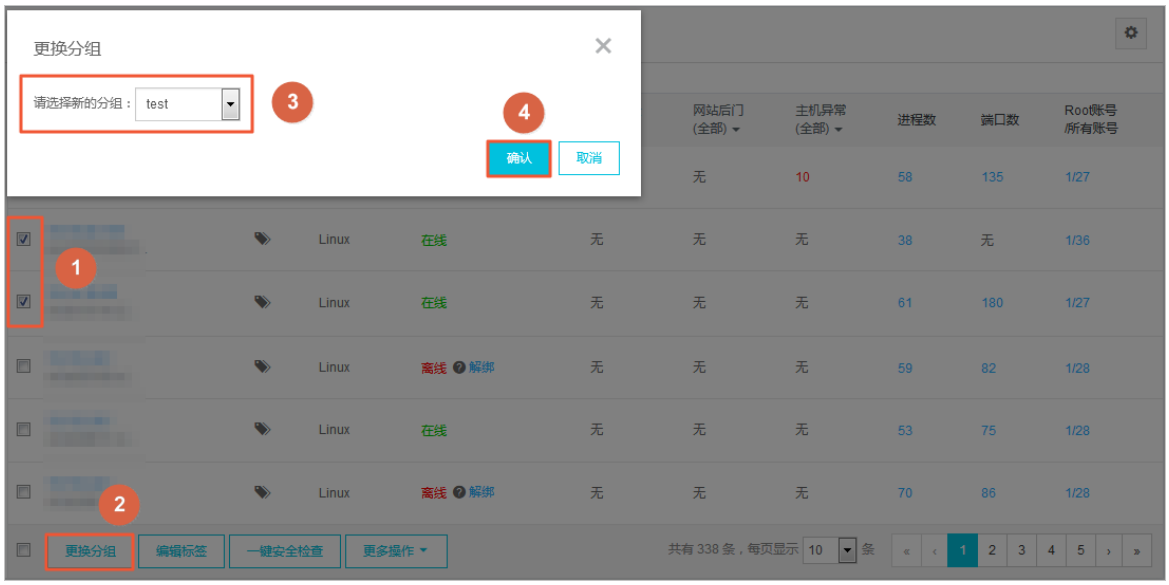
  单击子分组右侧的，输入子分组名称并单击**确认**。

- 删除子分组。

  单击子分组右侧的×，在弹出的确认框中单击**确认**。

  > **说明** 删除后该分组中的服务器默认移入**未分组**。

6. 给服务器进行分组。



   i. 在右侧的服务器列表中，选中服务器。
   ii. 单击**更换分组**。
   iii. 在弹出窗口的下拉菜单中选择分组。
   iv. 单击**确认**。

7.2.2. 管理主机列表

操作步骤

1. 请使用创建和授权的账号，登录云盾安全中心。

   创建和授权账号的具体操作，请参见创建和授权账号章节。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机列表**。
4.
5.
6.

7.3. 入侵事件

7.3.1. 入侵事件类型概述

主机安全支持敏感文件篡改、进程异常行为、网站后门、异常登录、恶意进程等安全告警类型，通过全面的安全告警类型帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

云盾安全中心可对您已开启的告警防御能力提供总览数据，帮助您快速了解已开启和未开启的防御项目。您可在**入侵事件**页面，查看安全告警的统计和防御项目的信息。

安全告警类型列表

防御项目包含的内容如下所示：

告警名称	告警说明
威胁情报	基于专有云云盾威胁情报，安骑士能够有效识别资产中的潜在威胁。威胁情报可以对威胁信息的相关内容进行关联、分析和处理，发现威胁后及时告警，从而提升威胁检查效率和响应速度。 • 恶意域名 • 恶意IP • 暗网通信IP • 中控通信IP • 矿池通信IP • 恶意URL • 恶意下载源

告警名称	告警说明
异常登录	检测服务器上的异常登录行为。通过设置合法登录IP、时间及账号，对于例外的登录行为进行告警。支持手动添加和自动更新常用登录地，对指定资产的异地登录行为进行告警。 可检测以下子项： • ECS非合法IP登录 • ECS在非常用地登录 • ECS登录后执行异常指令序列（SSH） • ECS被暴力破解成功（SSH）
网站后门	使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能： • Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。 • 支持针对网站后门检测的资产范围配置。 • 对发现的木马文件支持隔离、恢复和忽略。
精准防御	**病毒查杀**功能提供了精准防御能力，可对主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等类型进行防御。
异常账号	检测非合法的登录账号。
云产品威胁检测	检测其他云产品中是否存在威胁。
持久化后门	检测服务器上存在的可疑计划任务，对攻击者持久入侵用户服务器的威胁行为进行告警。
异常网络连接	检测网络显示断开或不正常的网络连接状态。
进程异常行为	检测资产中是否存在超出正常执行流程的行为。
恶意进程（云查杀）	采用云+端的查杀机制，对服务器进行实时检测，并对检测到的病毒文件提供实时告警。您可通过控制台对病毒程序进行处理。 可检测以下子项： • 访问恶意IP • 挖矿程序 • 自变异木马 • 恶意程序 • 木马程序
敏感文件篡改	检测是否存在对服务器中的敏感文件进行恶意修改，包含Linux共享库文件预加载配置文件的可疑篡改等行为。
其他	检测DDoS流量攻击等网络入侵行为。
Web应用威胁检测	检测通过Web应用入侵服务器的行为。
应用入侵事件	检测通过系统的应用组件入侵服务器的行为。

7.3.2. 查看和处理入侵事件

您可以在入侵事件页面查看和处理已检测出的告警事件。

背景信息

云盾检测出安全告警事件后，会在控制台**入侵事件**页面展示相关告警信息。如果告警事件未被处理，会展示在**入侵事件**页面的**待处理告警**列表中。告警事件处理完成后，将从**待处理告警**状态转化为**已处理**。

> **说明** 在**入侵事件**页面为您一直保留**待处理告警**和**已处理告警**记录。默认展示**待处理告警**记录。

查看告警事件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在入侵事件列表中，查看或搜索所有检测到的入侵和威胁告警及其详细信息。

处理告警事件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在**入侵事件**页面，定位到目标告警事件，单击**操作**栏的**处理**，对不同告警事件执行相应的处理后单击**立即处理**。

   > **说明** 如果告警事件包含多个关联异常，单击**处理**，会打开该告警事件的详情页面，您可对不同的异常事件分别进行处理。

   - **忽略**：忽略本次告警，该告警状态将变为**已处理**，后续不会再对该事件进行告警。
   - **加白名单**：如果告警为误报，您可以将本次告警加入白名单。告警加入白名单后该告警状态将变为**已处理**，后续安骑士不会再对该事件进行告警。您可以在**已处理**列表中定位到该事件对其进行**取消白名单**的操作。

     > **说明** 告警误报是指系统对正常程序进行告警。常见的告警误报有**对外异常TCP发包可疑进程**，提示您服务器上有进程在对其他设备发起了疑似扫描行为。

   - **同时处理相同告警**：对多个告警事件进行批量处理。批量处理告警事件前，请详细了解告警事件的信息。
5. （可选）如果您已确认一个或多个告警事件需要忽略或为误报，可在**入侵事件**页面，选中一个或多个告警事件，直接进行**忽略本次**或**加白名单**处理。

导出告警事件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。

4. 单击**入侵事件**页面危险等级栏  图标，导出报表。

   报表导出完成后，安全告警页面右上角会提示**导出完成**。

5. 在**安全告警处理**页面右上角**导出完成**对话框中，单击**下载**。
   安全告警事件文件会下载到本地。

7.3.3. 查看告警自动化关联分析

安骑士支持告警自动化关联分析。您可在安全告警列表页面单击单个告警事件名称进入告警自动关联分析页面，查看和处理告警事件所有关联的异常情况并进行攻击自动溯源，帮助您对告警事件进行全方位分析和便捷处理。

背景信息

- 告警自动关联分析功能可对相关的异常事件进行实时自动化关联，挖掘出潜藏的入侵威胁。
- 告警自动化关联以告警发生的时间顺序聚合成关联的告警，帮助您更便捷地分析和处理告警事件，提升您系统的应急响应机制。
- 告警自动化关联分析聚合后的告警以  图标标识。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在入侵事件列表中，单击目标**告警名称**打开告警事件详情面板。
5. 在告警事件详情面板，查看告警事件的详细信息、关联的异常事件和对告警的异常事件进行处理。
   - 查看告警详细信息

     您可查看受该告警事件影响的资产信息、告警首次发生或最新发生时间、关联异常事件的详情。
   - 查看受影响资产

     鼠标悬停在**受影响资产**名称上，会弹出对应资产的详情页面，方便您集中查看该资产的全部告警信息、漏洞信息、基线检查漏洞和资产指纹等信息。
   - 查看和处理**关联异常**

     您可在**关联异常**区域查看该告警事件关联的所有异常情况的详细信息和建议方案。
     - 单击各关联异常区域右侧的**备注**，可为该关联异常事件添加备注信息。
     - 单击备注信息右侧的 图标，即可删除备注信息。

7.3.4. 文件隔离箱

安骑士可对检测到的威胁文件进行隔离处理，被成功隔离的文件会添加到安全告警处理页面的文件隔离箱中。被成功隔离的文件可在30天内进行一键恢复，且隔离30天后系统将自动清除被隔离文件。本文介绍了如何查看隔离文件和解除文件隔离。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 在**入侵事件**页面单击右上角**文件隔离箱**。

   您可在**文件隔离箱**进行以下操作：

   - 在文件隔离箱列表中可以查看被隔离的文件主机地址、文件路径、状态和修改时间等信息。
   - 单击文件隔离箱页面右侧**操作**栏的**恢复**，可以将指定的被隔离文件从文件隔离箱中移除。恢复的文件将重新回到安全告警列表中。

7.3.5. 安全告警设置

安骑士的安全告警设置支持手动维护常用登录地和Web目录，并支持高级登录报警功能。

背景信息

安骑士提供高级登录报警功能，支持配置更精细的异常登录检测，例如设置合法登录的IP、时间、账号。

操作步骤

1.
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**入侵事件**。
4. 单击页面右上角**安全告警设置**。

   选择相应的功能页签，完成以下配置：

   - **添加常用登录地**

     a. 单击**常用登录地**右侧的**管理**按钮。

     b. 选中要添加的常用登录地点，然后选择添加应用的服务器。

     c. 单击**确定**，完成添加。

     安骑士支持**编辑**和**删除**已成功添加的常用登录地。

     - 单击目标常用登录地右侧的**编辑**，修改该登录地的生效服务器。
     - 单击目标常用登录地右侧的**删除**，删除该常用登录地配置。

   - **配置高级登录报警**

     > **说明** 配置高级登录告警，可进一步指定常用的登录IP、时间段和账号。配置完成后，安骑士会对指定外的登录情形进行告警。以下功能的操作类似**常用登录地**配置，可参考上文进行**添加**、**编辑**、**删除**。

     - 单击**常用登录IP**右侧的切换开关，打开或关闭登录IP检查，开启后通过非指定IP登录会触发报警。
     - 单击**常用登录时间**右侧的切换开关，打开或关闭登录时间检查，开启后在非指定时间登录会触发报警。
     - 单击**常用账号**右侧的切换开关，打开或关闭登录账号检查，开启后使用非指定账号登录会触发报警。

   - **自定义Web目录**

安骑士会自动检测您服务器资产中的Web目录，并进行动态检测和静态扫描；您也可以手动添加服务器中的其它Web目录进行检测扫描。

a. 单击**Web目录定义**右侧的**管理**。

b. 输入一个合法的Web路径，然后选中生效服务器，该路径将被添加到扫描路径的服务器。

> **说明** 出于性能效率考虑，不支持直接添加root目录作为Web目录。

c. 单击**确定**，完成添加。

7.3.6. 病毒云查杀

云盾安骑士病毒查杀（以下简称“云查杀”）集成了中国及中国以外地域多个主流的病毒查杀引擎，并利用阿里云海量威胁情报数据和自主研发的基于机器学习、深度学习异常检测模型，为用户提供全面和实时的病毒检测和防护服务。

目前云查杀每天检测数亿文件，实时服务百万云上服务器。

云查杀检测能力

安骑士采用云+端的查杀机制，客户端负责采集进程信息，上报到云端控制中心进行病毒样本检测。若判断为恶意进程，支持用户进行停止进程、隔离文件等处理。

云查杀具有以下检测能力：

- **深度学习检测引擎（自主研发）**：云盾深度学习检测引擎，使用深度学习技术，基于海量攻防样本，专门打造的一款适用于云环境的恶意文件检测引擎，智能识别未知威胁，是传统病毒查杀引擎的有力支撑。
- **云沙箱（自主研发）**：真实还原云上环境，监控恶意样本攻击行为，结合大数据分析、机器学习建模等技术，自动化检测和发现未知威胁，提供有效的动态分析检测能力。
- **集成中国及中国以外地域主流病毒查杀引擎**：云查杀集成中国及中国以外地域多款优秀的杀毒引擎，可对病毒库进行实时更新。
- **威胁情报检测**：基于云盾威胁情报数据，配合服务器异常行为检测模型，实现多维度检测异常进程和恶意行为。

云查杀覆盖的病毒类型

云查杀是阿里云安全技术与攻防专家经验融合的最佳实践，从数据的采集、脱敏、识别、分析、隔离到恢复，已形成安全闭环，同时支持用户在云盾控制台中对云查杀结果进行隔离和恢复处理。

云查杀覆盖以下病毒类型：

病毒类型	病毒描述
挖矿程序	非法占用服务器资源进行虚拟货币挖掘的程序。
蠕虫病毒	利用网络进行复制和传播的恶意程序，能够在短时间内大范围传播。
勒索病毒	利用各种加密算法对文件进行加密，感染此病毒一般无法解密，如WannaCry等。
木马程序	特洛伊木马，可受外部用户控制以窃取服务器信息或者控制权、盗用用户信息等的程序，可能会占用系统资源。
DDoS木马	用于控制肉鸡对目标发动攻击的程序，会占用本机带宽攻击其他服务器，影响用户业务的正常运行。

病毒类型	病毒描述
后门程序	黑客入侵系统后留下的恶意程序，通过该程序可以随时获得服务器的控制权或进行恶意攻击。
病毒型感染	运行后感染其他正常文件，将可能携带有感染能力的恶意代码植入正常程序，严重时可能导致整个系统感染。
恶意程序	其他威胁系统和数据安全的程序，例如黑客程序等。

云查杀的优势

- **自主可控**：基于自主研发的深度学习、机器学习能力及大数据攻防经验，并结合多引擎检测能力，为您提供全面、实时的病毒检测服务。
- **轻量**：Agent客户端仅占用1%的CPU、50 MB内存，不影响业务的运行。
- **实时**：获取进程启动日志，实时监控病毒程序的启动。
- **统一管理**：云安全中心控制台支持对所有服务器进行统一管理，实时查看所有服务器的安全状态。

安全威胁防御限制说明

云盾控制台支持安全告警实时检测与处理、漏洞检测与一键修复、攻击分析、云平台安全配置检查等功能，结合告警关联分析和攻击自动化溯源，帮助您全面加固系统和资产的安全防线。在云盾安骑士提供的防御能力以外，建议您定期更新服务器安全系统补丁、配合使用云防火墙、Web应用防火墙等产品缩小网络安全威胁的攻击范围，实时预防，不让黑客有任何可乘之机。

> **说明** 由于网络攻击手段、病毒样本在不断的演变，实际的业务环境也有不同差异，因此无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查、云平台配置检查等安全能力，提升整体安全防线，预防黑客入侵、盗取或破坏业务数据。

7.4. 主机指纹

7.4.1. 管理监听端口

本文介绍如何查看服务器的对外端口监听信息，便于您快速定位可疑监听行为。

背景信息

监听端口的应用场景包括：

- 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. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**资产指纹调查**页面，单击**端口**页签，查看所有**监听端口号**、**网络协议**和服务器信息。

   您可以通过搜索端口号、服务器进程名称、服务器名称或IP，快速查找端口。

在服务器信息列表中，查看服务器的**对应进程**、**IP**、**最新扫描时间**。

7.4.2. 管理软件版本

本文介绍如何定期查看、收集服务器的软件版本信息，便于您清点软件资产。

背景信息

软件版本的应用场景包括：

- 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.
2. 在控制台右上方，单击**安全**，选择**主机安全 > 安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**软件**页签查看所有使用中的**软件资产**和使用这些软件的**服务器数**。

   您可以使用软件名、版本、软件安装目录、服务器名称或IP进行搜索。
5. 单击软件名，查看其对应资产、软件版本等信息。

   单击右上角图标，下载软件版本数据表到本地，方便后续盘点资产。

7.4.3. 管理运行进程

本文介绍定期收集服务器的进程信息，并对变动情况进行记录的方法。便于进程清点和历史进程变动查看。

背景信息

运行进程的应用场景包括：

- 清点一个进程在哪些服务器中运行。
- 清点一台服务器运行了哪些进程。

操作步骤

1.
2.
3.
4. 单击**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**、**运行用户**、**启动参数**或**服务器名称或IP**进行搜索。
5. 单击进程名，查看进程对应资产、路径、启动参数等详细信息。

7.4.4. 管理账号信息

本文介绍定期收集服务器的账号信息，并对变动情况进行记录的方法。便于账号清点和历史账号变动查看。

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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**主机指纹**页面，单击**账户**页签。
5. 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、root权限、服务器名称或IP进行搜索。
6. 单击账号名，查看对应资产、root权限、用户组等详细信息。

7.4.5. 管理计划任务

本文介绍如何收集服务器计划任务，便于您清点任务。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**主机指纹**页面，单击**计划任务**页签。
5. 查看所有任务的路径和运行这些任务的主机数。
   您可以使用任务路径、服务器名称或IP进行搜索。
6. 单击任务路径，查看对应资产、执行命令、任务周期等详细信息。

7.4.6. 设置主机指纹采集频率

通过主机指纹设置功能，选择运行进程、系统账号、开放端口、软件版本数据的采集频率。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**主机指纹**。
4. 在**主机指纹**页面右上角单击**配置管理**。
5. 在相应项目的下拉菜单中，选择采集频率。
6. 单击**确定**，完成配置。

7.5. 日志检索

7.5.1. 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。

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

登录流水查询支持下表描述的字段。

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

暴力破解

暴力破解查询支持下表描述的字段。

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	攻击来源IP
warn_port	string	破解端口

字段	数据类型	说明
warn_user	string	破解用户名
warn_type	string	类型
warn_count	string	破解次数

进程启动日志

进程启动日志查询支持下表描述的字段。

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

端口监听快照

端口监听快照查询支持下表描述的字段。

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

字段	数据类型	说明
pid	string	进程ID
proc_name	string	进程名
proto	string	协议

账号快照

账号快照查询支持下表描述的字段。

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	账号超期时间
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

进程快照

进程快照查询支持下表描述的字段。

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1 MB不计算

网络连接日志

网络连接日志查询支持下表描述的字段。

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

7.5.2. 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。

语法逻辑说明

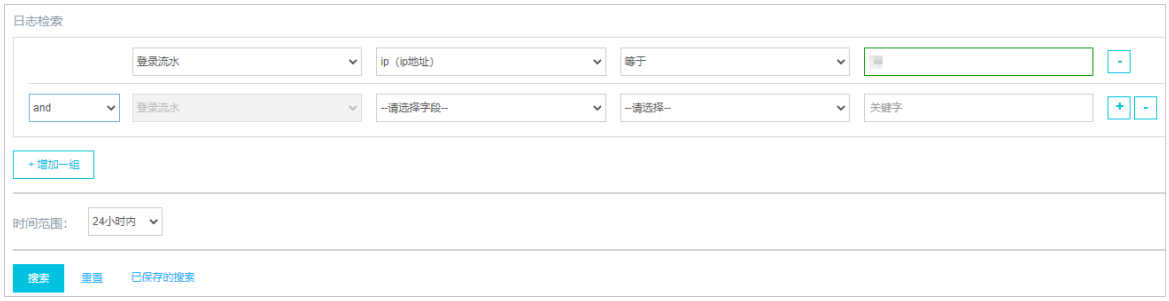
逻辑名称	描述
and	双目运算符。 形式为 `query 1 and query 2` ，搜索结果展示 `query 1` 和 `query 2` 查询结果的交集。 **说明** 如果多个单词间没有语法关键词，默认是and的关系。
or	双目运算符。 形式为 `query 1 or query 2` ，搜索结果展示 `query 1` 和 `query 2` 查询结果的并集。
not	双目运算符。 形式为 `query 1 not query 2` ，搜索结果展示符合 `query 1` 并且不符合 `query 2` 的结果，相当于 `query 1 - query 2` 。 **说明** 如果只有 `not query 1` ，那么表示从全部日志中选取不包含 `query 1` 的结果。

7.5.3. 查询日志

本文介绍如何搜索和查看主机日志。

操作步骤

1. 请使用创建和授权的账号，登录云盾安全中心。
   创建和授权账号的具体操作，请参见创建和授权账号章节。
2. 在控制台右上方，单击**安全**，在**主机安全**区域单击**安骑士**。
3. 在左侧导航栏，单击**日志检索**。
4. 设置日志检索条件。



说明 日志源、字段和语法逻辑说明，请参见各日志源字段说明和语法逻辑说明。

5. 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. 配置物理机安全

本文介绍了如何设置物理机的安全配置，包括周期性木马查杀和安骑士Agent工作模式。

操作步骤

1. 请使用创建和授权的账号，登录云盾安全中心。

   创建和授权账号的具体操作，请参见创建和授权账号章节。
2. 在左侧导航栏中，选择**物理机主机安全 > 设置**。
3. 配置对服务器进行周期性木马查杀。
   i. 单击**管理**。
   ii. 选择哪些服务器需要进行周期性的木马查杀。
   iii. 单击**确认**，完成配置。
4. 单击**管理**。

   设置服务器的防护模式。
   - **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。



8.应用安全

8.1. 快速入门

本文介绍如何快速使用Web应用防火墙WAF（Web Application Firewall）的功能。

WAF提出以智能语义分析算法解决Web攻击识别问题。通过WAF的智能分析算法，自主识别Web的攻击行为；同时结合学习模型，不断增强和完善分析能力，使其不依赖传统的规则库，即可满足用户日常安全防护需求。

WAF的使用流程如下：

1. 定制WAF的防护规则。

   WAF提供默认的防护策略，同时用户也可以根据自身的业务特点，灵活定制防护策略。

   - 配置防护策略，请参见配置防护策略。
   - 配置自定义规则，请参见配置自定义规则。
   - 配置CC防护规则，请参见配置CC防护规则。
2. 添加防护的网站。

   WAF支持防护面向互联网的网站和面向内网的网站。

   - 添加面向互联网提供服务的网站，请参见添加防护站点。
   - 添加面向内网提供服务的网站，请参见添加VPC防护站点。
3. 设置DNS解析。

   将原来DNS解析的网站源IP修改为WAF的虚拟IP，请参见修改DNS解析。
4. 查看WAF防护结果。
   - 查看防护的整体信息，请参见查看防护总览。
   - 查看访问状态信息，请参见查看访问状态监控。
   - 查看Web攻击检测日志，请参见查看攻击检测日志。
   - 查看CC攻击防护日志，请参见查看CC防护日志。

8.2. 防护总览

8.2.1. 查看防护总览

本文介绍如何查看WAF的防护总览。

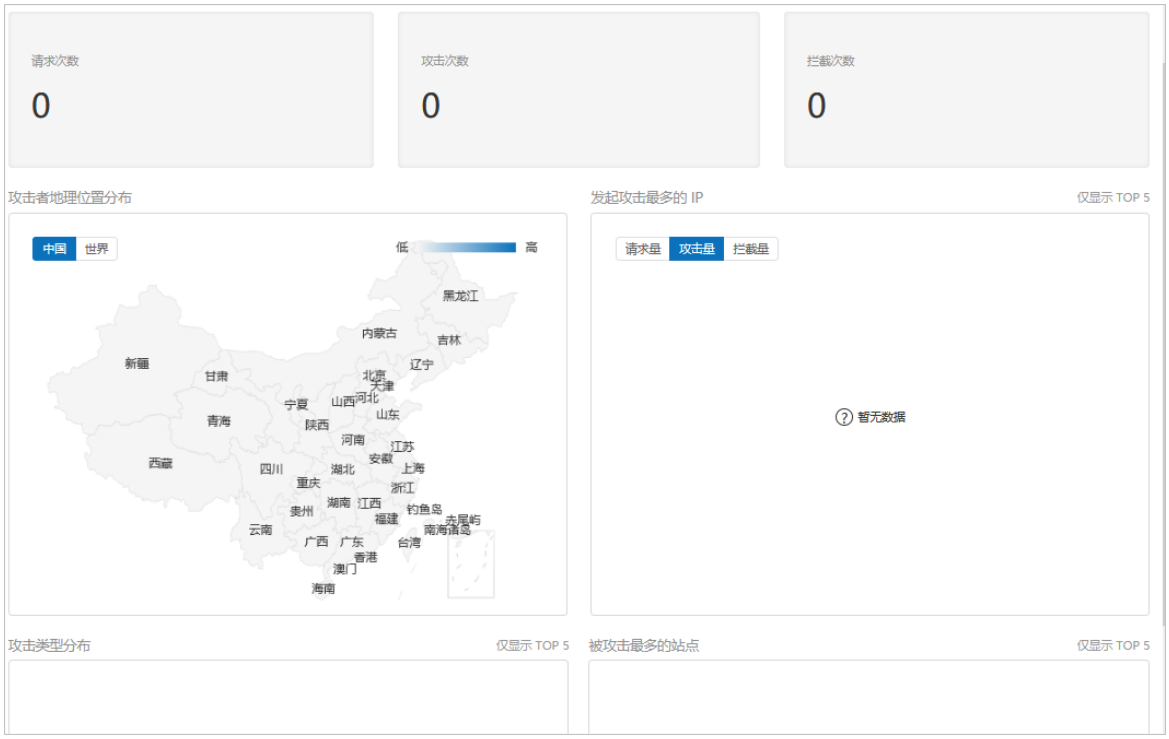
背景信息

防护总览展示WAF对历史攻击数据的统计信息，攻击源IP地理信息分布，防护状态展示等情况。管理者通过总览，快速了解Web防护情况，并制定相应的规则和措施保护Web安全。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，单击**防护总览**。

4. 在**防护总览**页面，查看**最近24小时统计**和**最近30天统计**的WAF防护情况。



- 请求次数

  显示总的请求次数。

- 攻击次数

  显示总的攻击次数。

- 拦截次数

  显示总的拦截次数。

- 攻击者地理位置分布（地图形式）

  在地图上展示攻击者的分布情况，支持查看中国和世界地图。

  展示请求次数和拦截次数。

- 发起攻击最多的IP（仅显示Top 5）

  以条形图展示Top 5发起攻击最多的IP地址。横坐标为请求次数，纵坐标为IP地址。

- 攻击类型分布（仅显示Top 5）

  以条形图展示Top 5的攻击类型的分布占比和各攻击类型的次数。

- 被攻击最多站点（仅显示Top 5）

  以条形图展示Top 5被攻击站点和各站点的次数。

8.2.2. 查看访问状态监控

本文介绍如何查看访问状态的监控信息。

背景信息

通过访问状态监控，了解Web服务的访问情况，分析业务访问情况，帮助安全管理员及时发现业务漏洞，提

升防御能力。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护总览 > 访问状态监控**。
4. 筛选需要查看的访问状态，查看访问详情。



8.3. 防护日志

8.3.1. 查看攻击检测日志

本文介绍如何查看攻击检测日志。

背景信息

通过攻击检测日志，分析Web服务的受攻击情况，根据分析结果更新防护策略和自定义规则、处理Web服务漏洞等，提升Web服务的安全性。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护日志 > 攻击检测日志**。
4. 单击**筛选**，设置筛选条件，单击**确定**。

   > **说明** 筛选条件中的多个条件，是与的关系。即需要满足所有条件才能生效。

5. 在列表中查看攻击检测结果。

8.3.2. 查看CC防护日志

本文介绍如何查看CC防护日志。

背景信息

通过CC防护日志，分析Web服务的受到的CC攻击情况，根据分析结果更新CC防护规则和CC白名单、处理Web服务漏洞等，提升Web服务的安全性。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。

3. 在左侧导航栏，选择**防护日志 > CC防护日志**。
4. 单击**筛选**，设置筛选条件，单击**确定**。

   > **说明** 筛选条件中的多个条件，是与的关系。即需要满足所有条件才能生效。

5. 在列表中查看CC攻击检测结果。

   列表展示CC攻击的日志内容、关联的规则和发生的时间。

8.3.3. 查看BOT验证日志

本文介绍了如何查看BOT验证日志。

背景信息

通过BOT验证日志，可分析Web服务的受到的BOT攻击情况，根据分析结果更新BOT防护策略，提升Web服务的安全性。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**应用安全 > Web应用防火墙**。
3. 在**Web应用防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，在选择**Web应用防护 > 防护日志 > BOT验证日志**。
5. 在**BOT验证日志**，单击**验证结果日志**或**验证记录日志**。

   日志列表展示了BOT攻击的日志内容、验证结果、策略名称、源IP发生的时间等信息。

相关文档

- 配置BOT防护

8.3.4. 查看系统操作日志

本文介绍如何查看系统操作日志。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护日志 > 系统操作日志**。
4. 在列表中查看系统操作日志。

   列表展示用户名、内容、IP地址、创建时间。

8.3.5. 查看访问日志

本文介绍如何查看访问日志。

操作步骤

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护日志 > 访问日志**。
4. 单击**筛选**，设置筛选条件，单击**确定**。

> **说明** 筛选条件中的多个条件，是与的关系。即需要满足所有条件才能生效。

5. 在列表中查看访问日志。

   列表展示请求访问地址、目的IP、源IP、方法、响应码及时间。

8.4. 防护配置

8.4.1. 配置防护策略

本文介绍如何配置WAF的防护策略。

背景信息

WAF提供默认的防护策略，同时用户也可以根据自身的业务特点，灵活定制防护策略。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护配置 > 攻击防护策略**。
4. 单击**添加防护策略**，在文本框中输入**策略名称**，单击**确定**。
5. 单击新增的防护策略**操作**列的 图标，查看防护策略规则。



参数	说明
解码方式	选择解码的算法类型。
攻击检测模块	设置该防护策略启动哪些攻击检测类型，及其阈值。

参数	说明
拦截方式	设置拦截时显示的错误码和图片。
HTTP响应检测	设置**启用HTTP响应检测**开启状态和**允许检测的Body长度上限**的阈值。
HTTP 请求检测	设置**允许检测的Body长度上限**的阈值。
检测超时限制	设置**启用超时检测**开启状态和**检测超时时间**的阈值。

以修改**攻击检测模块**为例，设置步骤如下：

i. 鼠标移动到**攻击检测模块**的具体模块上（以**SQL注入检测模块**为例），单击**修改**图标。

ii. 在**SQL注入检测模块**对话框中，设置检测参数。

参数	说明
是否启用	是否使用该模块提供检测功能。
阻断阈值	提供**不阻断**、**仅阻断高危**、**阻断中危及高危**、**阻断全部**选项。
记录日志阈值	提供**不记录**、**仅记录高危**、**记录中危及高危**、**记录全部**选项。
检测非注入型SQL	是否开启检测非注入型SQL攻击。

iii. 单击**确定**。

6. 管理防护策略。

   如果某个防护策略已经不需要保留，可以选中该防护策略，选择**更多操作 > 删除选中防护策略**并在提示框中单击**确定**删除该策略。

   > **说明** 系统默认策略不能删除。

8.4.2. 配置自定义规则

本文介绍如何配置WAF的自定义规则。

背景信息

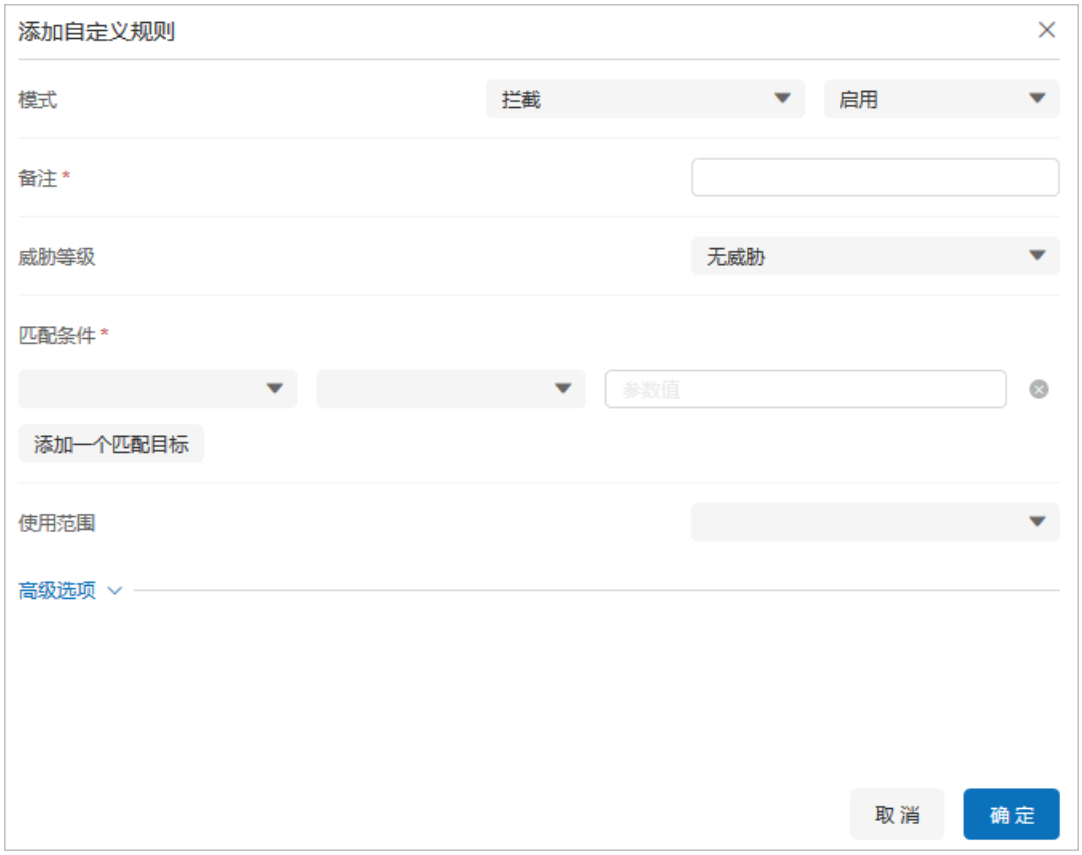
自定义规则便于满足各个企业对入侵检测的不同标准设置，在此管理员可以自行添加、编辑或删除入侵检测规则。使用规则可以灵活地过滤一部分指定的请求。

多条自定义规则之间是**或**的关系。如果存在两条自定义规则，其触发条件一致，但拦截、放行等动作不同，则系统按照从上到下的排列顺序匹配上方的规则。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。

3. 在**Web应用防护**界面左侧导航栏，选择**防护配置 > 自定义配置**。
4. 单击**添加规则**，在**添加自定义规则**中，设置规则参数。



自定义规则配置项

参数	说明
模式	设置自定义规则的工作模式，支持**拦截**、**放行**、**观察**、**检查模块控制**四种模式。 ○ **拦截**：如果HTTP请求符合自定义规则，则拦截该请求。 ○ **放行**：如果HTTP请求符合自定义规则，则放行该请求。 ○ **观察**：如果HTTP请求符合自定义规则，则记录并放行该请求。 ○ **检查模块控制**
备注	设置自定义规则的备注信息，一般说明该规则的防护目的。
威胁等级	包含**无威胁**、**低危**、**中危**、**高危**。
匹配条件	设置自定义规则的匹配条件。 单击**添加一个匹配目标**，可以设置多个匹配条件。多个匹配条件间是**与**的关系，即需要满足所有匹配条件，自定义规则才能生效。
使用范围	选择自定义规则保护的站点。
是否记录日志	命中时是否记录日志，默认处于开启状态。开启后，拦截记录均会记录在入侵检测日志中。

参数	说明
攻击类型	定义该自定义规则针对的是哪种攻击类型。
过期时间	设置该自定义规则过期时间。

5. 单击**确定**，创建自定义规则。
6. 管理自定义规则。
   - 编辑自定义规则

     在某个自定义规则的**操作**栏，单击 图标，修改自定义规则。

   - 启用自定义规则

     如果某个自定义规则是禁用状态，如果需要重新开启，则选中该规则，在**更多操作**下拉列表中，选择**启用选中规则**。

   - 禁用自定义规则

     如果某个自定义规则是启用状态，现在不需要使用了，则选中该规则，在**更多操作**下拉列表中，选择**禁用选中规则**。

   - 导出自定义规则

     如果您想导出某个自定义规则，则选择该规则，在**更多操作**下拉列表中，选择**导出选中规则**。

   - 删除自定义规则

     如果某个自定义规则不再需要使用，则选中该规则，在**更多操作**下拉列表中，选择**删除选中规则**。

8.4.3. 配置CC防护规则

本文介绍如何配置CC防护规则，用于拦截CC攻击。

背景信息

CC（HTTP Flood）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。

创建CC防护规则

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护配置 > CC防护**。
4. 单击**添加规则**，进入**添加CC防护规则**页面。
5. 设置CC防护规则，单击**确定**。



参数	说明
规则模式	设置CC防护规则的工作模式，支持**观察模式**、**阻断模式**。 ○ 阻断模式：限制满足访问控制规则的请求。 ○ 观察模式：对满足访问控制规则的请求信息进行日志记录，不生效限制动作。
规则类型	设置CC防护规则的类型，包含**限制满足条件的用户**、**限制已知的用户**，两者区别在于是否为确定的IP、SESSION 。 ○ **限制满足条件的用户**：访问控制规则为设置 触发的条件对满足条件的用户进行限制生效。可配置项包含：**触发限制的条件**、**访问次数的统计范围**、**限制方式**、**限制时间**以及**访问数据统计范围**（高级选项）。 ○ **限制已知的用户**：按照设置的限制规则来限制已知的用户，需要配置对应的限制的IP、SESSION列表以及限制的方式，配置完成后按照对应的限制规则生效。
规则名称	设置CC防护规则的名称。

参数	说明
受限制目标的类型	设置限制的访问来源类型：**IP**、**SESSION**。 **说明** 如果**受限制目标的类型**选择SESSION，则启用该CC规则的防护站点，需要在**用户识别**中选择**WAF用户系统**，具体操作，请参见添加互联网防护站点。
触发限制的条件	当**受限制目标的类型**选择**限制满足条件的用户**时，需要设置CC防护规则的触发条件。
访问次数的统计范围	当**受限制目标的类型**选择**限制满足条件的用户**时，需要设置CC防护规则保护的访问目的地址。 ○ **限制用户访问以某个地址为前缀的地址** ○ **限制用户访问某个地址** ○ **统计用户访问所有地址**
要限制的IP列表、要限制的SESSION列表	当**受限制目标的类型**选择**限制已知的用户**时，根据**受限制目标的类型**，设置需要限制的IP或者SESSION列表，每行设置一个。
限制访问的地址	当**受限制目标的类型**选择**限制已知的用户**时，设置CC防护规则保护的访问目的地址。 ○ **限制用户访问以某个地址为前缀的地址** ○ **限制用户访问某个地址** ○ **限制用户访问所有地址**
限制方式	如果访问来源触发了限制条件，采取的限制方式。 ○ **封禁**：禁止访问来源访问目的地址。 ○ **限制频率**：限制访问来源访问目的地址的频率。
限制时间	设置限制行为生效的时间。
访问数据统计范围	当**受限制目标的类型**选择**限制满足条件的用户**时，高级选项下表示配置访问统计数据源的范围： ○ 统计全量访问数据：配置全量访问数据后，对于所有经由WAF的满足频率限制条件的用户都会触发限频动作，但对系统性能有一定的消耗。 ○ 统计TOP访问数据：配置TOP访问数据范围后，限频生效范围仅限于统计信息中的TOP数据（生效范围是实时访问监控中显示的TOP 100数据 ），默认为该配置项对于性能消耗相对较小（当全量数据范围大于TOP 100时）。

管理CC防护规则

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护配置 > CC防护**。

4. 在规则列表中，管理、编辑已添加的CC防护规则。
   - 搜索CC防护规则

     单击**筛选**，在**筛选**面板中添加过滤条件，可用于快速定位CC规则。
   - 启用CC防护规则

     如果某个CC防护规则是禁用状态，如果需要重新开启，则选中该规则，选择**更多操作 > 启用选中规则**。
   - 禁用CC防护规则

     如果某个CC防护规则是启用状态，现在不需要使用了，则选中该规则，选择**更多操作 > 禁用选中规则**。
   - 删除CC防护规则

     如果某个CC防护规则不再需要使用，则选中该规则，选择**更多操作 > 删除选中规则**。

8.4.4. 配置CC白名单

本文介绍如何配置CC白名单。

背景信息

如果确定访问用户的安全性，可以将用户添加到CC白名单中，后续CC防护规则将不会拦截该用户的访问。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在**Web应用防护**界面左侧导航栏中，选择**防护配置 > CC防护**。
4. 在**CC白名单**页签，单击**添加一个不受限制的用户**，添加白名单用户，单击**确定**。



参数	说明
类型	设置白名单用户的类型：**IP**、**SESSION**。
IP或SESSION	根据**类型**，设置白名单用户的IP或者SESSION列表，每行设置一个。
备注	白名单说明。

5. 管理已添加的CC白名单。
   - 搜索CC白名单

     选择**筛选 > 添加一个筛选条件**，添加过滤条件，可用于快速定位CC白名单。
   - 删除CC白名单

     如果某个CC白名单不再需要使用，则选中该规则，选择**更多操作 > 删除选中的用户**。

8.4.5. 配置BOT防护

本文介绍了如何配置BOT防护规则，用于防护机器人程序的流量。

背景信息

BOT防护通过识别机器人流量和网页代码，可以对爬虫、恶意注册、暴力破解、薅羊毛等恶意网络行为进行检测防护。

创建BOT防护

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**应用安全 > Web应用防火墙**。
3. 在**Web应用防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**Web应用防护 > 防护配置 > BOT防护**。
5. 在**BOT防护**页面，单击**添加BOT防护策略**。
6. 在**添加BOT防护**面板，完成以下配置，单击**确定**。



参数	说明
BOT策略状态	设置BOT策略的状态。可选项： ○ 开启：表示启用该策略。 ○ 关闭：表示禁用该策略。

参数	说明
策略名称	设置BOT策略的名称。
配置使用站点	选择BOT策略使用的站点。您可以选择**互联网侧站点**或**VPC侧站点**，可勾选多个站点。 注意 当您有配置多个策略生效地址的需求，单击**策略生效地址**可添加多条。
配置策略生效地址	配置BOT策略的生效地址范围。您可以选择**前缀匹配**、**正则匹配**或**完全匹配**。
端口设置	配置策略生效地址的端口。 注意 自动添加已选站点中的端口。当您有配置其他端口的需求时，单击**添加一组端口**完成端口配置。
忽略搜索引擎	勾选需要忽略的搜索引擎流量，避免正常的搜索受到防护策略影响。
人机验证	设置开启或关闭人机验证功能。
匹配特征	设置人机验证的匹配规则。
验证方式	设置人机验证的验证方式。可选项： ○ 浏览器验证 ○ 验证码
验证失效时长	配置人机验证通过后的有效期。
是否记录日志	配置人机验证是否记录日志。可选项： ○ 记录验证日志 ○ 不记录验证日志 注意 选择**记录验证日志**，可在**防护日志 > BOT验证日志**查看具体的日志详情。

启用、禁用、删除BOT防护

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**应用安全 > Web应用防火墙**。
3. 在**Web应用防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**Web应用防护 > 防护配置 > BOT防护**。
5. 在**BOT防护**页面，勾选目标策略，启用、禁用或删除选中策略。

您也可以单击**操作**列**编辑**，修改目标策略的配置参数。

8.4.6. 上传证书

本文介绍了如何上传证书。

背景信息

在**证书管理**页面上传证书后，您在**防护站点列表**页面配置站点时，可以选择已上传的证书。

> **说明** 证书和域名具有对应关系，在**防护站点列表**中配置SSL时，域名需要选择对应的证书。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**应用安全 > Web应用防火墙**。
3. 在**Web应用防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**Web应用防护 > 防护配置 > 证书管理**。
5. 在**证书管理**页面，上传新的证书。
   i. 单击**SSL证书**、**国密证书CA证书**或**国密CA证书**。
   ii. 在页面右上角，单击**上传证书**按钮。
   iii. 在**证书名称**文本框中，设置**证书名称**。
   证书名称建议填写对应的域名，便于识别管理。
   > **注意** 如果您在上传SSL证书时，证书和私钥在同一个文件中，请选中**证书文件中包含私钥**。
   iv. 在**证书文件**区域，将证书文件和私钥文件分别拖到对应位置。
   v. 设置**证书密码**。
   > **注意** 只有当您在上传SSL证书且未选中**证书文件中包含私钥**，才需要配置该参数。
   vi. 单击**确定**，完成证书的上传。
6. （可选）删除已上传的证书。
   如果已上传的证书过期，您可以删除该证书。
   i. 在证书列表中，选中需要删除的证书。
   ii. 选择**更多操作 > 删除选中的SSL证书**。
   iii. 在确认对话框中，单击**确定**。

8.4.7. 添加互联网防护站点

本文介绍了如何在WAF上添加面向互联网的防护站点。

背景信息

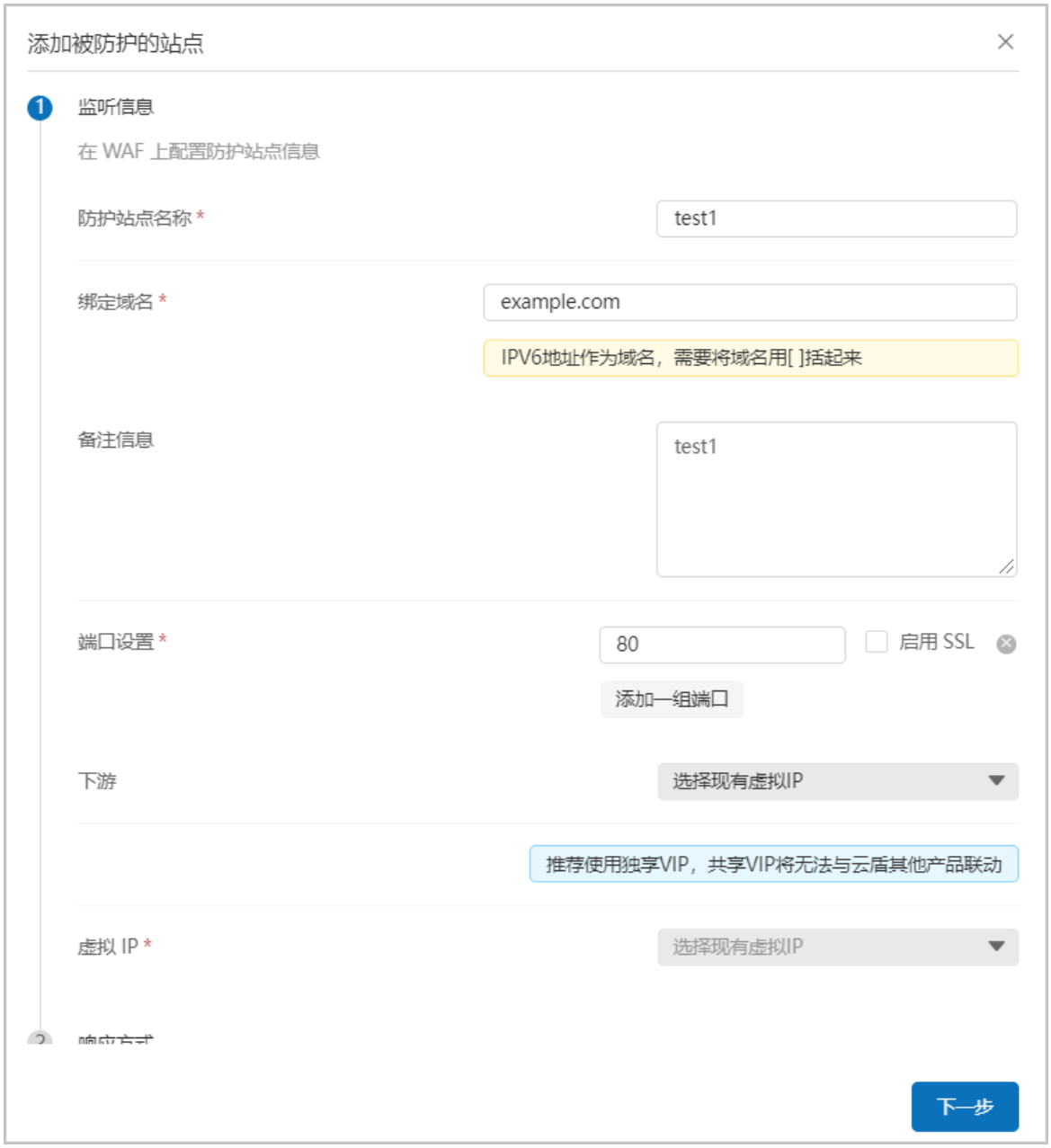
WAF支持防护面向互联网的站点和面向内部网络的站点。

- 关于如何设置面向互联网的站点，请参见本章节。
- 关于如何设置面向内部网络的站点，请参见添加VPC防护站点。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**应用安全 > Web应用防火墙**。
3. 在**Web应用防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**Web应用防护 > 防护配置 > 防护站点管理**。
5. 在**防护站点管理**页面，单击**互联网侧站点**。
6. 在**互联网侧站点**页签，单击**添加站点**。
7. 在**添加被防护的站点**面板的**监听信息**区域，完成参数配置，单击**下一步**。

   设置需要WAF进行防护的网站地址，WAF支持HTTP和HTTPS类型网站。

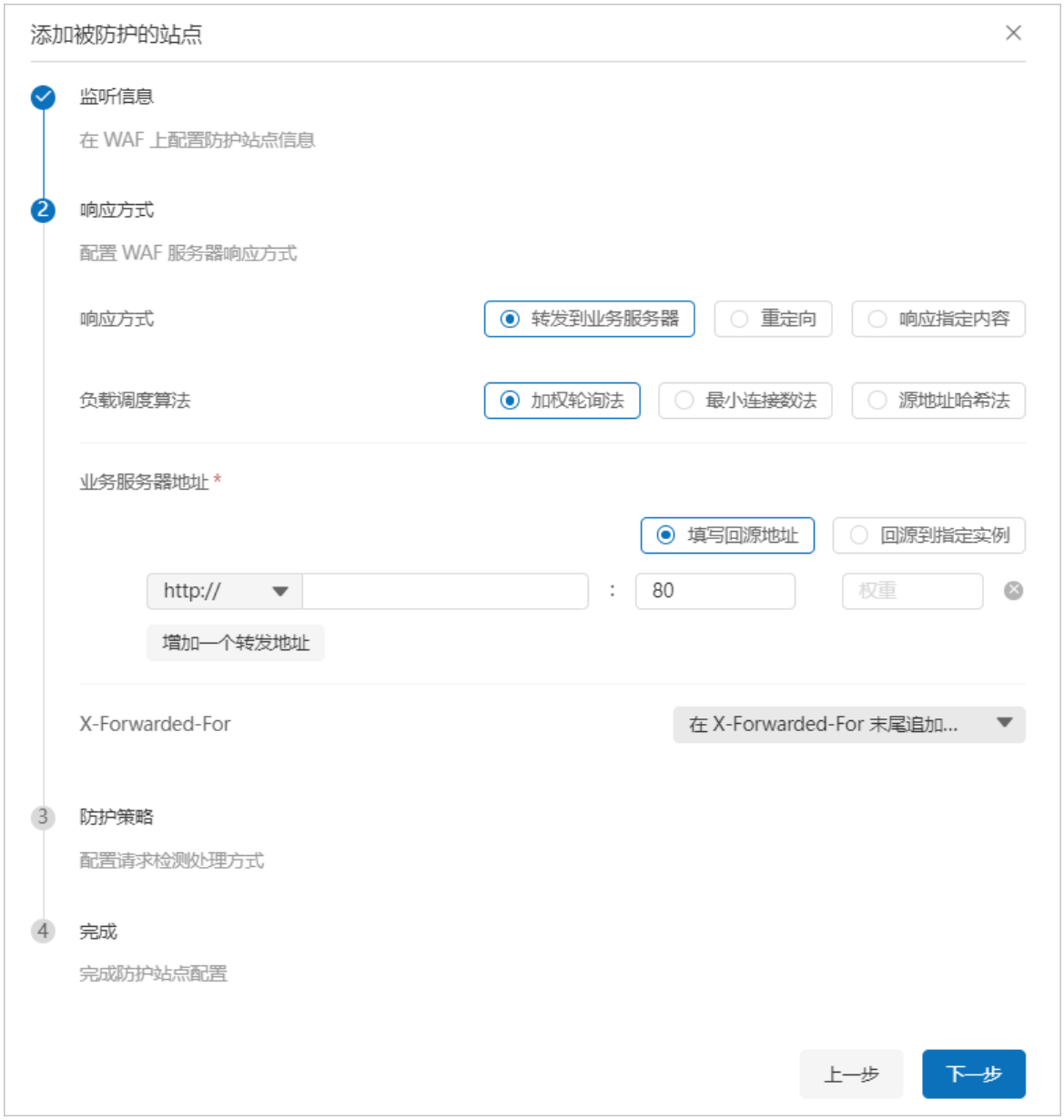


参数	说明
防护站点名称	设置防护站点名称。
绑定域名	设置防护站点域名。 ○ 可使用星号（*）作通配。 ○ 多个域名可使用逗号（,）分隔。
端口设置	设置WAF监听防护的端口。 ○ 如果站点支持HTTPS访问，可选中**启用SSL**并上传HTTPS证书。 ○ 如果站点支持多个端口访问，单击**添加一组端口**新增其他端口。

参数	说明
证书方案	设置网站的证书方案。默认勾选**SSL证书**，您可以根据实际情况勾选**国密证书**。 **注意** 只有在**端口设置**中选择**启用SSL**，才需要设置本参数。
SSL证书设置	设置网站的HTTPS证书，可选*上传一个新证书*或*选择一个已有的证书*。 - *上传一个新证书*：如果网站使用的HTTPS证书以前没有上传到WAF，选择此选项。 默认情况下HTTPS证书和私钥分开上传，如果选中**证书文件中包含私钥**，则只需要上传一个文件。 - *选择一个已有的证书*：如果网站使用的HTTPS证书以前有上传到WAF，选择此选项，并在下拉菜单中选择网站HTTPS证书。 **注意** 只有在**端口设置**中选择**启用SSL**，才需要设置本参数。
证书名称	设置证书名称。 **注意** 只有在**端口设置**中选择**启用SSL**且上传一个新证书，才需要设置本参数。
SSL证书文件	上传HTTPS证书和密钥。 默认情况下HTTPS证书和私钥分开上传，如果**HTTPS证书**中选中**证书文件中包含私钥**，则只需要上传一个包含了HTTPS证书和私钥的文件。 **注意** 只有在**监听端口**中选择**启用SSL**且上传一个新证书，才需要设置本参数。
国密证书设置	设置网站的国密证书，请选择**上传一个新证书**或**选择一个已有的证书**： - **上传一个新证书**：如果网站使用的国密证书以前没有上传到WAF，选择此选项。 - **选择一个已有的证书**：如果网站使用的国密证书以前有上传到WAF，选择此选项，并在下拉菜单中选择网站国密证书。 **注意** 只有在**端口设置**中勾选**启用SSL**且在**证书方案**中勾选**国密证书**，才需要设置本参数。
国密证书文件	上传国密证书和密钥。 **注意** 只有在**端口设置**中勾选**启用SSL**且在**证书方案**中勾选**国密证书**，才需要设置本参数。

参数	说明
下游	选择下游的虚拟IP是现有虚拟IP或是需创建虚拟IP。可选项： ○ 选择现有虚拟IP ○ 创建虚拟IP ○ 创建指定虚拟IP
虚拟IP	选择具体的虚拟IP。 **注意** 默认最多选择8个虚拟IP地址，只有在**下游**中选择**选择现有虚拟IP**，才需设置本参数。
虚拟IP类型	选择虚拟IP类型。可选项： ○ 外网经典网络IP ○ 内网经典网络IP **注意** 只有在**下游**中选择**创建虚拟IP**或**创建指定虚拟IP**，才需设置本参数。
虚拟IP协议	选择虚拟IP协议。可选项： ○ ipv4 ○ ipv6 **注意** 只有在**下游**中选择**创建虚拟IP**，才需设置本参数。
是否指定机房	设置指定的虚拟IP是否有指定的机房。可选项： ○ 是 ○ 否 **注意** 只有在**下游**中选择**创建指定虚拟IP**，才需设置本参数。
自定义IP	自定义虚拟IP地址。 **注意** 只有在**下游**中选择**创建指定虚拟IP**且在**是否指定机房**中选择**否**，才需设置本参数。
所属机房名称	选择虚拟IP指定机房的名称。 **注意** 只有在**下游**中选择**创建指定虚拟IP**且在**是否指定机房**中选择**是**，才需设置本参数。

8. 在**添加被防护的站点**面板的**响应方式**区域，完成参数配置，单击**下一步**。



响应方式	参数	说明
转发到业务服务器	**负载调度算法**	选择负载均衡算法，支持**加权轮询法**、**源地址哈希法**、**最小连接数法**。
	业务服务器	流量经过WAF后转发到业务服务器，支持**填写回源地址**和**回源到指定实例**。 ○ **填写回源地址**：直接填写回源的业务服务器地址，如果有多个业务服务器，则根据**负载调度算法**做负载均衡。 ○ **回源到指定实例**：回源到指定的ECS或SLB，如果有多个业务服务器，则根据**负载调度算法**做负载均衡。

响应方式	参数	说明
	源IP透传选项	设置源IP透传方式。 X-Forwarded-For位于HTTP协议的请求头，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。
重定向	**响应状态码**	流量经过WAF后重定向到指定地址。 重定向响应状态码可选择**301**、**302**、**307**和**308**。 ○ **301**：表示请求的网页已永久移动到新位置。 ○ **302**：表示服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。 ○ **307**：服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。 ○ **308**：永久重定向。
	重定向地址	输入重定向后的URL地址。
响应指定内容	**响应状态码**	流量经过WAF后响应指定内容。 响应状态码可选择**200**、**400**、**401**、**402**、**404**、**405**、**500**、**503**、**504**等。
	响应内容	上传响应的内容。 例如设置为**响应指定内容**，并在此上传一张图片。如果用户访问该网站后，会返回此图片。

9. 在**添加被防护的站点**面板的**防护策略**区域，完成参数配置，单击**下一步**完成配置，单击**完成**。

> **注意** **响应方式**只有设置为**转发到业务服务器**模式，才能设置防护策略。

参数	说明
防护策略	选择WAF的防护策略，默认选择**默认防护策略**。更多信息，请参见配置防护策略。
用户识别	设置是否使用用户识别功能。 **说明** 如果此被防护站点启用了CC防护，而且CC防护规则中**受限制目标的类型**选择SESSION，则**用户识别**需要选择**WAF用户系统**。

8.4.8. 添加VPC防护站点

本文介绍了如何在WAF上添加专有云的VPC防护站点。

背景信息

WAF支持防护面向互联网的站点和面向内部网络的站点。

- 关于如何设置面向互联网的站点，请参见添加防护站点。
- 关于如何设置面向内部网络的站点，请参见本章节。

操作步骤

1.
2. 在顶部菜单栏，将光标放置在**安全**上，选择**应用安全 > Web应用防火墙**。
3. 在**Web应用防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**Web应用防护 > 防护配置 > 防护站点管理**。
5. 在**防护站点管理**页面，单击**VPC侧站点**。
6. 在**VPC侧站点**页签，单击**添加站点**。
7. 在**添加被防护的站点**面板的**监听信息**区域，完成参数配置，单击**下一步**。

   设置需要WAF进行防护的VPC站点，WAF支持HTTP和HTTPS类型网站。

参数	说明
防护站点名称	设置防护站点名称。
绑定域名	设置防护站点域名： ○ 可使用星号（*）作通配。 ○ 多个域名可使用半角逗号（,）分隔。
端口设置	设置WAF监听防护的端口： ○ 如果站点支持HTTPS访问，选中**启用SSL**并上传HTTPS证书。 ○ 如果站点支持多个端口访问，单击**增加一个需要监听的端口**新增其他端口。
证书方案	设置网站的证书方案。默认勾选**SSL证书**，您可以根据实际情况勾选**国密证书**。 **注意** 只有在**端口设置**中选择**启用SSL**，才需要设置本参数。
SSL证书设置	设置网站的SSL证书，请选择**上传一个新证书**或**选择一个已有的证书**： ○ **上传一个新证书**：如果网站使用的HTTPS证书以前没有上传到WAF，选择此选项。 默认情况下HTTPS证书和私钥分开上传，如果选中**证书文件中包含私钥**，则只需要上传一个文件。 ○ **选择一个已有的证书**：如果网站使用的HTTPS证书以前有上传到WAF，选择此选项，并在下拉菜单中选择网站HTTPS证书。 **注意** 只有在**端口设置**中选择**启用SSL**，才需要设置本参数。

参数	说明
证书名称	设置证书名称。 **注意** 只有在**端口设置**中选择**启用SSL**，才需要设置本参数。
SSL证书文件	上传SSL证书和密钥。 默认情况下SSL证书和私钥分开上传，如果在**证书名称**中选中**证书文件中包含私钥**，则只需要上传一个包含了SSL证书和私钥的文件。 **注意** 只有在**端口设置**中勾选**启用SSL**，才需要设置本参数。
国密证书设置	设置网站的国密证书，请选择**上传一个新证书**或**选择一个已有的证书**： ○ **上传一个新证书**：如果网站使用的国密证书以前没有上传到WAF，选择此选项。 ○ **选择一个已有的证书**：如果网站使用的国密证书以前有上传到WAF，选择此选项，并在下拉菜单中选择网站国密证书。 **注意** 只有在**端口设置**中勾选**启用SSL**且在**证书方案**中勾选**国密证书**，才需要设置本参数。
国密证书文件	上传国密证书和密钥。 **注意** 只有在**端口设置**中勾选**启用SSL**且在**证书方案**中勾选**国密证书**，才需要设置本参数。

8. 在**配置VPC区域**，完成参数配置，单击**下一步**。

参数	说明
被防护VPC	选择防护站点所属的VPC。
下游	可选择以下方式 ○ **选择现有虚拟IP** ○ **负载均衡 SLB** ○ **创建虚拟 IP** **注意** 请确保在**系统设置 > 全局系统设置**页面，已打开**私有SLB作为站点下游**开关，才支持**负载均衡SLB**选项。
交换机选择	选择防护站点所属的虚拟交换机。
负载均衡 SLB	选择防护站点所属的SLB。

参数	说明
创建虚拟IP方式	选择**选择现有虚拟IP**或**创建虚拟IP**。
VPC虚拟IP	○ 当**创建虚拟IP方式**选择**选择现有虚拟IP**时，在**VPC虚拟IP**中选择已有的虚拟IP地址。 注意 默认最多选择8个虚拟IP地址。 ○ 当**创建虚拟IP方式**选择**创建虚拟IP**时，在**VPC虚拟IP**中单击**点击生成虚拟IP**。

9. 设置负载调度的响应方式，单击**下一步**。

响应方式	参数	说明
转发到业务服务器	**负载调度算法**	选择负载均衡算法，支持**加权轮询法**、**源地址哈希法**、**最小连接数法**。
	业务服务器	流量经过WAF后转发到业务服务器，支持**填写回源地址**和**回源到指定实例**。 ○ **填写回源地址**：直接填写回源的业务服务器地址，如果有多个业务服务器，则根据**负载调度算法**做负载均衡。 ○ **回源到指定实例**：回源到指定的ECS或SLB，如果有多个业务服务器，则根据**负载调度算法**做负载均衡。
	X-Forwarded-For	设置源IP透传方式。 X-Forwarded-For位于HTTP协议的请求头，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。
重定向	**响应状态码**	流量经过WAF后重定向到指定地址。 重定向响应状态码可选择**301**、**302**和**307**。 ○ **301**：表示请求的网页已永久移动到新位置。 ○ **302**：表示服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。 ○ **307**：服务器目前从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。
	重定向地址	输入重定向后的URL地址。
响应指定内容	**响应状态码**	流量经过WAF后响应指定内容。 响应状态码可选择**200**、**404**、**503**等。
	响应内容	上传响应的内容。 例如设置为**响应指定内容**，并在此上传一张图片。如果用户访问该网站后，会返回此图片。

10. 设置防护策略，单击**完成**。

参数	说明
防护策略	选择WAF的防护策略，默认选择**默认防护策略**。更多信息，请参见配置防护策略。
用户识别	设置是否使用用户识别功能。

8.4.9. 本地验证域名接入配置

本文介绍了如何本地验证域名接入配置结果。

背景信息

在把业务流量切到WAF之前，建议先通过本地验证的方式确保配置正常，WAF转发正常。在本地hosts文件中添加虚拟IP和域名后，本地在使用浏览器访问被防护域名时，访问请求会先经过WAF。

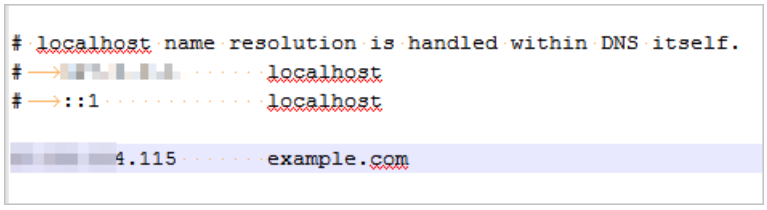
操作步骤

1.
2. 在本地PC的*hosts*文件中添加虚拟IP和域名。

   以Windows 7为例，hosts文件路径为*C:\Windows\System32\drivers\etc\hosts*。

   i. 使用记事本等文本编辑器打开hosts文件。

   ii. 在最后一行添加 `<WAF的虚拟IP><被防护站点>` 。

   > **说明** 域名前面的IP为WAF分配的虚拟IP。

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WAF的虚拟IP，如果依然解析到源站IP，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WAF的接入配置正确，则能够正常访问网站。

5. 验证WAF保护功能。

   模拟一个测试的Web攻击请求，确认WAF是否能够阻断访问。

   例如，在域名的URL后添加 `/?alert(xss)` ，如 `www.example.com/?alert(xss)` 。此时，WAF应能弹出阻拦页面。

8.4.10. 修改DNS解析

本文介绍了通过修改DNS解析到WAF，完成业务正式接入。

背景信息

完成本地验证，确认没有问题之后，则可以修改DNS解析，把业务流量切到WAF。

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的虚拟IP，实现WAF防护接入。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**防护配置 > 防护站点管理**。
4. 单击防护站点**操作**列的 图标。
5. 在**基本信息**页签中，记录下防护站点的虚拟IP。
6. 登录域名解析服务商的控制台，定位到对应域名的域名解析设置，将A记录的值改为防护站点的虚拟IP。

> **说明** 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。

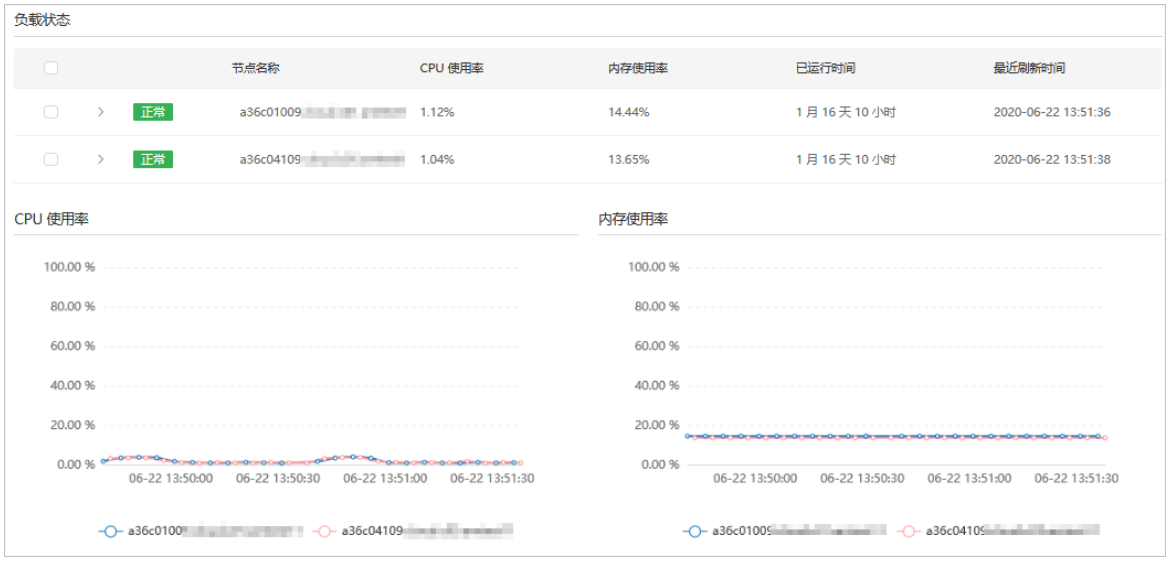
8.5. 系统管理

8.5.1. 查看节点负载状态

本文介绍如何查看WAF节点的CPU和内存的负载情况。通过查看结果，识别问题故障或判断是否需要进行扩容。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在**Web应用防护**界面左侧导航栏中，选择**系统信息 > 节点状态**。
4. 在**负载状态**页签，查看WAF各节点的负载状态。



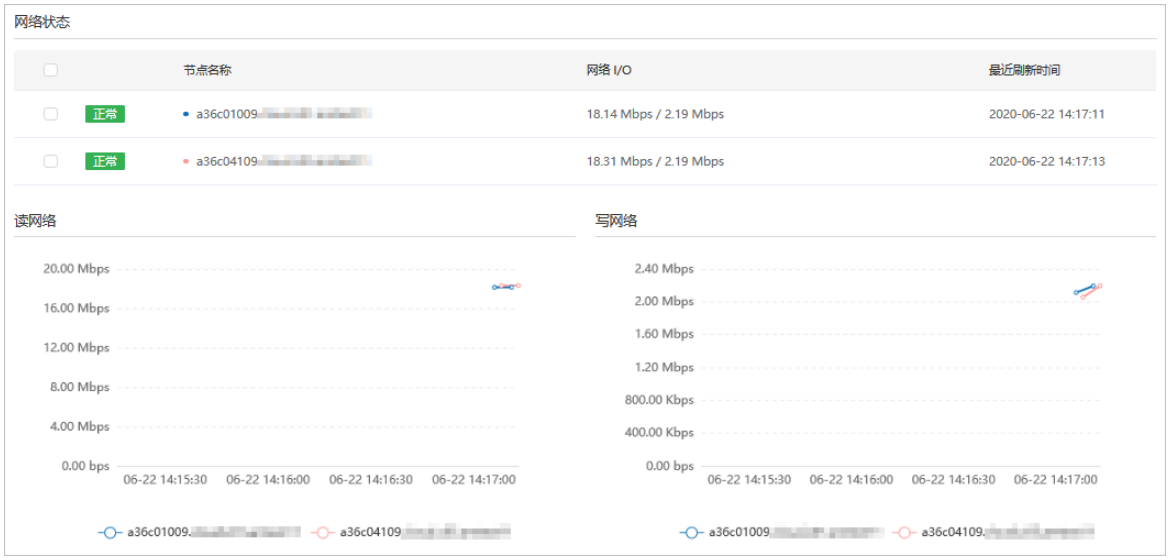
在该页面可以查看各节点的CPU和内存使用率，并在页面下方以图表形式展示一段时间内的使用率变化情况。

8.5.2. 查看节点网络状态

本文介绍如何查看WAF节点的网络状态，包括网络I/O、流量检测和流量转发状态。

节点网络状态

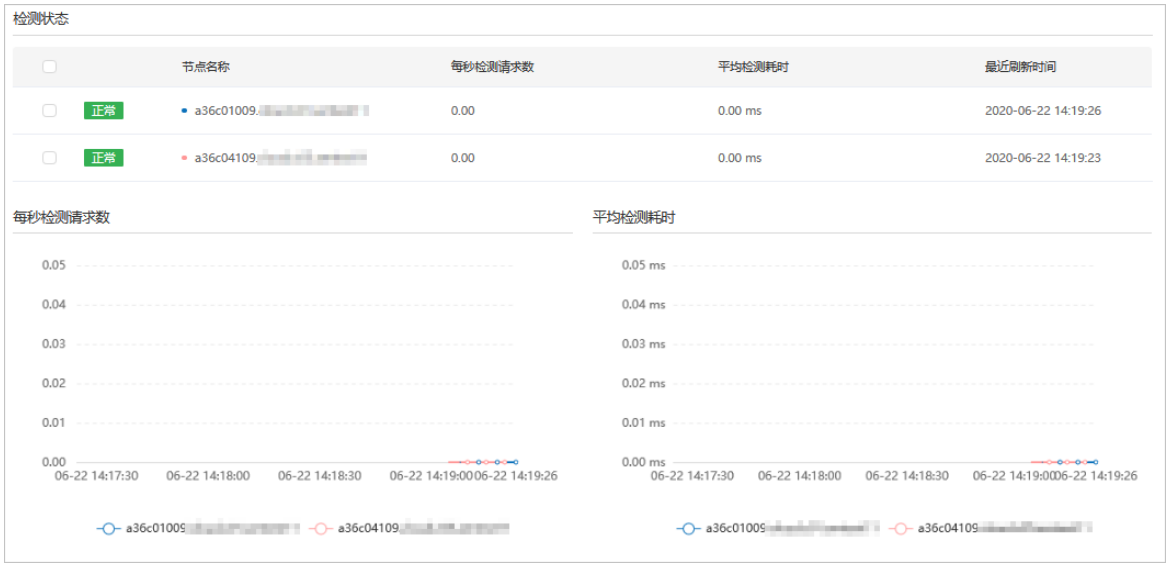
1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**系统信息 > 节点状态**。
4. 在**节点状态**页面，单击**网络状态**页签。
5. 查看WAF节点的网络I/O情况。



流量检测状态

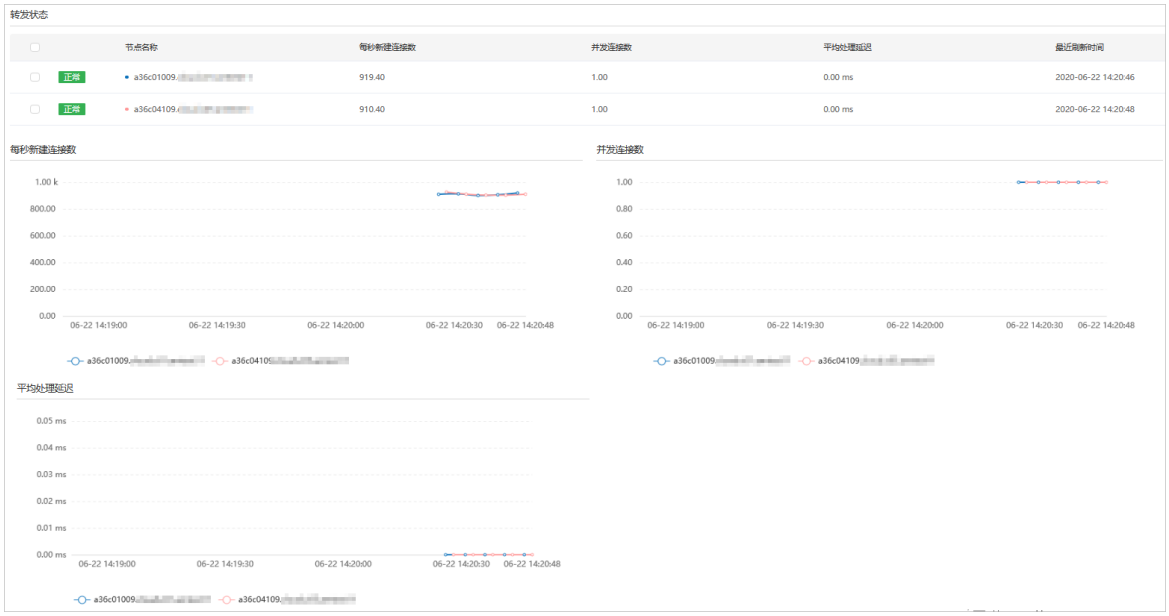
1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**系统信息 > 节点状态**。
4. 在**节点状态**页面，单击**检测状态**页签。
5. 查看WAF节点的网络流量检测状态。



流量转发状态

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**系统信息 > 节点状态**。
4. 在**节点状态**页面，单击**转发状态**页签。
5. 查看WAF节点的网络流量转发状态。



8.5.3. 查看节点磁盘状态

本文介绍如何查看WAF的节点的磁盘状态。通过查看结果，识别问题故障或判断是否需要进行扩容。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**系统信息 > 节点状态**。
4. 单击**磁盘状态**页签，查看WAF各节点的磁盘状态。



在该页面可以查看各节点的磁盘I/O和磁盘使用率，并在**读磁盘**和**写磁盘**区域以图表形式展示一段时间内磁盘的读写变化情况。

8.5.4. 配置告警服务

本文介绍如何在WAF添加Syslog服务器。添加后，WAF的告警日志可以通过Syslog协议方式推送到Syslog服务器。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。
3. 在左侧导航栏，选择**系统设置 > 告警配置**。
4. 在**告警服务配置**页签，单击**添加告警服务**。
5. 在**添加告警服务**对话框中，设置Syslog服务器参数。



参数	说明
SYSLOG服务器	设置Syslog服务器的地址和端口号。
RFC	选择Syslog协议标准，支持**RFC3164**和**RFC5424**。
协议	选择传输协议，支持**TCP**和**UDP**。
备注	设置Syslog说明信息，方便后续的识别和管理。
通用	设置告警类型，支持系统管理和系统监控和告警。
安全	选择需要发送Syslog日志的模块。

6. 单击**确定**，新添加的Syslog服务器将显示在Syslog列表中。
7. 在新添加Syslog服务器的**操作**栏，单击 图标测试告警是否能够正常发送。
   - 如果显示**发送告警测试成功**，则表示添加Syslog服务器成功。
   - 如果显示报错信息，则表示WAF与Syslog服务器无法连接，例如下图所示。



8.5.5. 配置告警阈值

本文介绍如何配置告警阈值。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**应用安全**区域单击**Web应用防火墙**。

3. 在左侧导航栏，选择**系统设置 > 告警配置**。
4. 在**告警阈值配置**页签，单击需要修改的阈值后面的图标。
5. 在编辑对话框中，设置对应的告警阈值。



阈值	说明
每秒查询数	当每秒查询数超过设置的阈值上报告警，当每秒查询数设置为0不上报告警。
新建连接数	新建连接数过高不告警。
CPU使用率过高	CPU使用率连续一段时间内超过一定百分比发送告警信息。
内存使用率过高	内存使用率连续一段时间内超过一定百分比发送告警信息。
磁盘使用率过高	磁盘使用率超过一定百分比发送告警信息。

6. 单击**确定**，完成告警阈值设置。

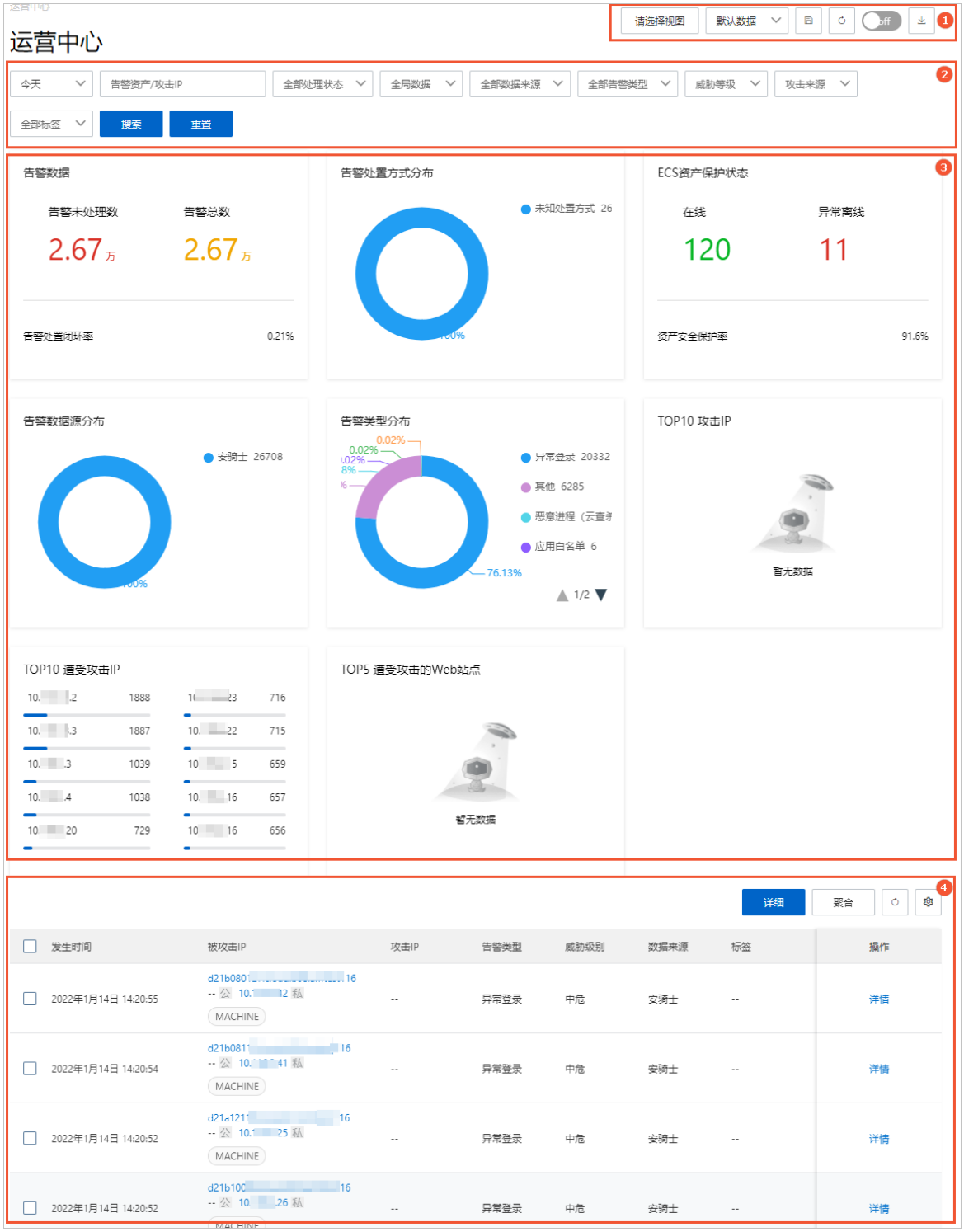
9.云安全管理中心（SOC）

9.1. 运营中心

本文展示专有云数据安全的详细信息，安全管理员通过此功能了解网络被攻击及防御的整体情况，以便后续提升网络安全性能。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**运营中心**。
4. 在**运营中心**页面，查看以下运营数据。


运营中心
请选择视图
默认数据
今天
告警资产/攻击IP
全部处理状态
全局数据
全部数据来源
全部告警类型
威胁等级
攻击来源
全部标签
搜索
重置
告警数据
告警未处理数
2.67 万
告警总数
2.67 万
告警处置闭环率
0.21%
告警处置方式分布
未知处置方式 26
ECS资产保护状态
在线
120
异常离线
11
资产安全保护率
91.6%
告警数据源分布
安骑士 26708
告警类型分布
异常登录 20332
其他 6285
应用白名单 6
76.13%
1/2
TOP10 攻击IP
暂无数据
TOP10 遭受攻击IP
TOP5 遭受攻击的Web站点
暂无数据
详细
聚合
发生时间
被攻击IP
攻击IP
告警类型
威胁级别
数据来源
标签
操作
2022年1月14日 14:20:55
2022年1月14日 14:20:54
2022年1月14日 14:20:52
2022年1月14日 14:20:52
MACHINE
异常登录
中危
安骑士
详情

功能	说明	支持的操作

功能	说明	支持的操作
菜单栏（图示①）	设置运营中心为您展示的数据。	○ 设置展示项：单击下拉框，设置您要在视图中展示的数据分类。 默认显示**告警数据**、**告警处置方式分布**、**ECS资产保护状态**、**告警风险级别**、**告警数据源分布**、**告警类型分布**、**TOP 10攻击IP**、**TOP 10遭受攻击IP**、**TOP 5遭受攻击的Web站点**以及**列表展示区**。您可以根据实际情况设置需要显示的数据。 ○ 数据来源：单击下拉框，设置数据的来源。 ○ 保存视图：单击  图标，保存当前视图。 ○ 手动刷新数据：单击  图标，手动刷新当前视图的数据。 ○ 自动刷新数据：启动  图标，系统会每5分钟自动刷新当前视图的数据。 ○ 导出数据：单击  图标，导出当前视图的数据。
查询条件区域（图示②）	设置运营中心数据的查询条件。 您可以根据**查询时间**、**告警资产/攻击IP**、**处理状态**、**全局数据**、**全部数据来源**、**全部告警类型**、**威胁登记**、**攻击来源**、**标签**来设置查询条件。	单击条件的下拉框，根据实际情况，设置数据的查询条件，然后单击**搜索**。 如果设置过程中，需要重新设置，可以单击**重置**重新设置。
查询结果区域（图示③）	查询结果区域与查询条件区域联动显示，系统根据您设置的查询条件，显示查询的结果信息。	无。

功能	说明	支持的操作
列表详情区域（图示④）	列表详情区域与查询条件区域联动显示，系统会根据您设置的查询条件，显示您的数据被威胁的详细列表。	○ 设置数据显示方式： ■ 单击**详细**，系统会根据时间顺序为您显示所有被攻击IP的详细信息。 ■ 单击**聚合**，系统将被攻击IP、攻击IP、告警威胁相同，且以10分钟为一个周期，满足的告警数据聚合在一起，为您显示详细信息。 ○ 查看数据详情：单击目标数据右侧操作列的**详情**，展开**详情**面板，查看该条数据被威胁及防御的详细信息。 ○ 添加标签：单击**批量添加标签**，设置标签信息，方便您后续直接定位该类问题。 ○ 刷新列表数据：单击 图标，手动刷新列表数据。 ○ 设置列表展示项：单击 ，设置列表的展示项，默认为全选。

9.2. 态势监控

本文展示专有云网络环境的安全信息，安全管理员通过此功能了解网络整体安全情况。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**仪表盘**。
4. 在**仪表盘**页面的右上角，**时间统计**下拉框中可以选择统计时间。

   时间统计支持**近24小时**、**近7日**和**近30日**。
5. 根据查询时间，查看目标时间段内网络安全整体信息。



仪表盘主要展示以下网络安全信息。

- 展示**新发现网络攻击**、**新发现异常行为**、**新发现脆弱性**和**当前防护组织数**的统计数据。
- 展示**TOP 5遭受攻击组织**、**TOP 5待处理异常行为**、**TOP 5待处理脆弱性组织**、**ECS保护状态**数据。
- 展示租户侧和平台侧的**安全趋势**。
- 展示**最新异常行为**、**异常行为类型分布**、**新增资产分布**数据。
- 展示**最新网络攻击**、**网络攻击类型分布**、**防护总资产分布**数据。

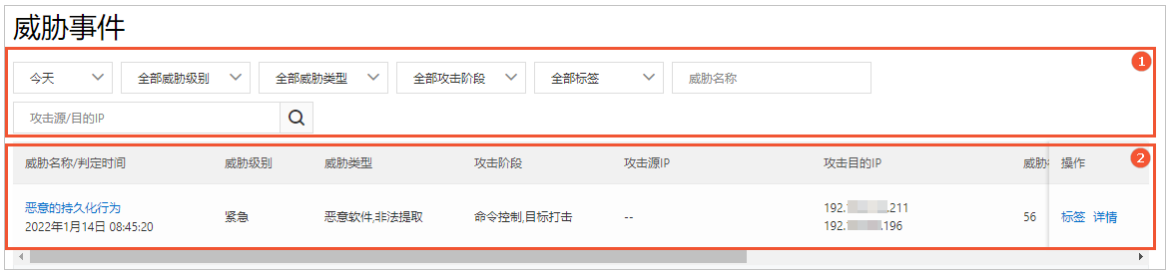
9.3. 风险分析

9.3.1. 查看威胁事件

本文为你介绍如何查看威胁事件，帮助安全管理员快速定位威胁详情，保障网络安全。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云安全管理中心 SOC**。
3. 在左侧导航栏，选择**风险分析 > 威胁事件**。
4. 在**威胁事件**页面，查看威胁事件详情。



功能	说明	支持的操作
查询条件区域（图示①）	设置威胁事件的查询条件。 您可以根据**查询时间**、**威胁级别**、**威胁类型**、**攻击阶段**、**标签**、**威胁名称**、**攻击源/目的IP**来设置查询条件。	在查询条件下拉框中选择待查询的信息，或者输入关键字，然后单击 图标。 如果您不设置查询条件，默认显示所有威胁事件。
查询结果区域（图示②）	查询结果区域与查询条件区域联动显示，系统根据您设置的查询条件，显示查询的威胁事件信息。	○ 查看威胁事件的详细信息：单击目标**威胁名称**或者右侧操作列的**详情**，进入目标威胁事件页面， 查看具体的**威胁信息**和**证据信息**。 ○ 为威胁事件添加标签：单击右侧操作列的**标签**，您可以为威胁事件自定义标签，方便您后续定位到该事件。

查看**威胁信息**：在**威胁信息**页签，查看威胁事件**开始时间**、**最后检测时间**、**检测规则**、**网络协议**、**威胁情报**，以及**源信息**、**目的信息**、**关键信息**。

查看**证据信息**：在**证据信息**页签，查看威胁事件的原始日志。

9.3.2. 查看弱点分析数据

本文介绍如何查看平台侧和租户侧的弱点分析数据，帮助安全管理员准确定位风险问题。

查看平台侧弱点分析结果

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云安全管理中心 SOC**。

3. 在左侧导航栏，选择**风险分析 > 弱点分析**。
4. 在**弱点分析**页面，单击**平台**。
5. 在**平台基线**页签，设置平台基线风险的过滤条件，然后单击 图标。

> **说明** 如果不设置任何查询条件，默认显示所有平台基线。

过滤条件	说明
威胁等级	选择需要查看的平台基线风险的威胁等级。
处理状态	选择平台基线风险的处理状态 。
起始和结束时间	设置要查询的时间范围。
检查项目名称	通过输入平台基线风险名称的关键字，搜索相关结果。

查询到的所有结果显示在平台基线列表中，您可以根据业务需要，执行如下操作。

- 单击 图标，刷新平台基线列表。
- 单击 图标，导出平台基线列表。

查看租户侧弱点分析结果

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**风险分析 > 弱点分析**。
4. 在**弱点分析**页面，单击**租户**。
5. 在**租户**页签，单击**漏洞**或者**主机配置**页签。
   - **漏洞**：漏洞的信息。
   - **主机配置**：主机配置基线风险的信息。
6. 设置漏洞（或主机配置基线风险）查询条件，然后单击 图标。

> **说明** 如果不设置任何查询条件，默认显示所有漏洞（或主机配置基线风险）。

过滤条件	说明
组织	选择漏洞（或主机配置基线风险）涉及资产所属的组织。
等级	选择需要查看的漏洞（或主机配置基线风险）的威胁等级。
处理状态	选择漏洞（或主机配置基线风险）的处理状态 。
起始和结束时间	设置需要查询的时间范围。

过滤条件	说明
名称、资产、CVE编号搜索	通过输入漏洞（或主机配置基线风险）名称、受影响资产或CVE编号的关键字，搜索相关结果。

查询到的所有结果显示在平台页签的列表中，您可以根据业务需要，执行如下操作。

- 单击 图标，刷新漏洞（或主机配置基线风险）列表。
- 单击 图标，导出漏洞（或主机配置基线风险）列表。

9.3.3. 查看流量分析数据

本文介绍如何查看全局流量的分析信息，包括均值流量、峰值流量、平均流量趋势图、租户和平台流量信息。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云安全管理中心 SOC**。
3. 在左侧导航栏，选择**风险分析 > 流量分析**。
4. 在**流量分析**页面，查看全局流量信息。

   支持查看的信息如下所示：
   - 查看流量均值和峰值。
     a. 在**流量分析**页面左上角，选择需要查看的周期和方向。

        周期可选值：**近6小时**、**近24小时**、**近7天**。

        流量方向可选值：**入方向**、**出方向**。

     b. 在页面左上方，查看所选周期内指定方向流量的均值和峰值。
   - 查看流量趋势图。
     a. 在**流量分析**页面左上角，选择流量类型。
     b. 在趋势图上查看周期内，各类型流量整体趋势。
   - 在**租户流量**页签，查看租户的流量信息列表。
   - 在**平台流量**页签，查看平台的流量信息列表。

9.3.4. 查看威胁情报

本文介绍如何查看您的资产在近30天内已遭受威胁的整体情况和统计数据。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云安全管理中心 SOC**。
3. 在左侧导航栏，选择**风险分析 > 威胁情报**。
4. 在**概览**页面，查看威胁情报服务检测到的专有云已遭受的威胁事件和统计数据。

您可以执行以下操作：

- 搜索任意IP，确认其是否为恶意来源。

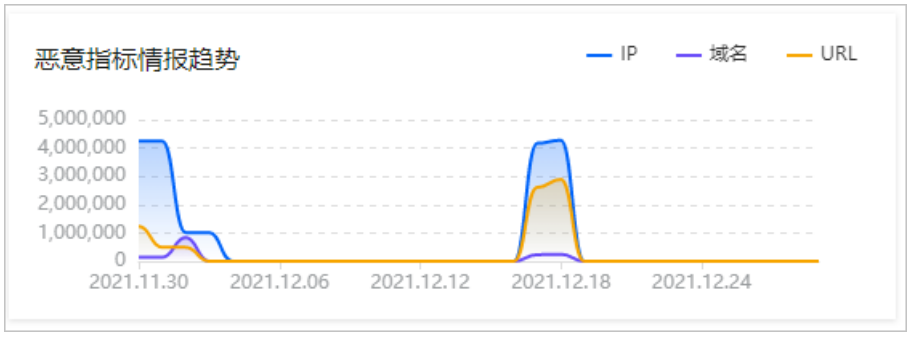
  在右上角的搜索框中输入您需要排查的IP，单击图标。在**云安全管理中心（SOC） > 威胁情报 > IP搜索**页面显示**IP报告**查看报告详细信息。

- 查看**恶意指标情报总数**。

  在**恶意指标情报总数**区域，查看检测到的专有云遭受的威胁情况，包括恶意IP总数、恶意域名总数、恶意URL总数。



- 查看**恶意指标情报趋势**。



- 查看**威胁情报调用总结**。

  在**威胁情报调用总结**区域，查看**威胁情报使用指标**、**威胁IOC查询类型**、**威胁情报标签分布**及**威胁情报查询统计**。



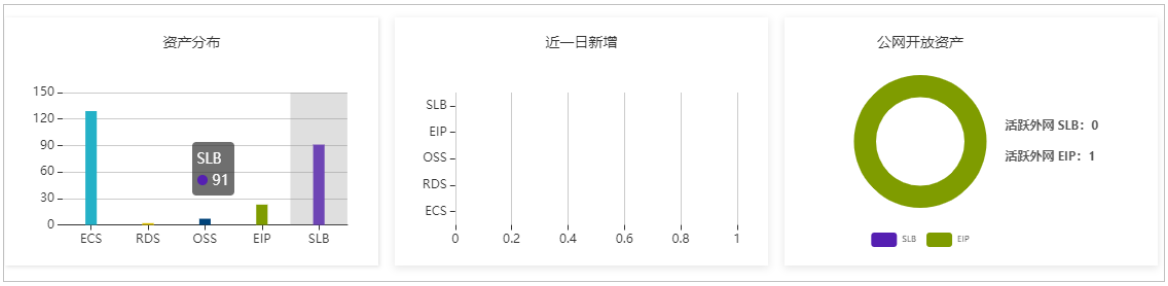
9.4. 资产管理

9.4.1. 查看租户资产

本文介绍如何查看租户侧资产信息，包括ECS、RDS、OSS、SLB和EIP等资产。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云安全管理中心 SOC**。
3. 在左侧导航栏，选择**资产管理 > 租户资产**。
4. 在**租户资产**页签，您可以查看**资产分布**、**近一日新增**以及**公网开放资产**的统计数据。



5. 选择目标资产（例如**云主机（ECS）**），设置搜索项搜索资产信息。

   您也可以在搜索栏中输入指定的IP地址、实例名称直接查询目标资产信息。



> **说明** 如果您不设置任何查询条件，则默认显示全部资产。

搜索项	说明
组织	选择资产所属的组织。
VPC	选择资产具体的VPC。
状态	选择资产目前运行的状态。
是否新增	选择资产是否为新增的资产。
自动快照风险	选择资产自动快照风险的等级。
服务器名称或IP	输入服务器名称或者IP。

6. 在资产列表中查看资产信息。

   如果您需要导出查询到的资产信息，请单击 图标。

9.4.2. 查看平台资产

本文介绍如何查看平台侧资产的物理机防护信息，安全管理员通过异常行为定位问题并获取对应的处理建议。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**资产管理 > 平台资产**。
4. 在**平台资产**的**物理机防护**页签，搜索目标资产。

   查询结果显示在平台资产列表中。

   > **说明** 默认显示全部资产信息。



5. 单击目标资产名称，查看该资产**物理机防护**和**异常行为**的详细信息。

   物理机防护信息



   异常行为信息



   如果异常信息较多，您可以根据**数据来源**、**提醒**、**可疑**、**紧急**、**处理状态**、**告警类型**、**起始和结束日期**进行筛选。

如果处理目标告警信息时，单击该**告警名称**，展开**告警详情**面板，您可以查看**受影响资产**、**发生时间**、**结束时间**，并在**关联的异常**中查看详细信息及处理建议。



9.5. 日志管理

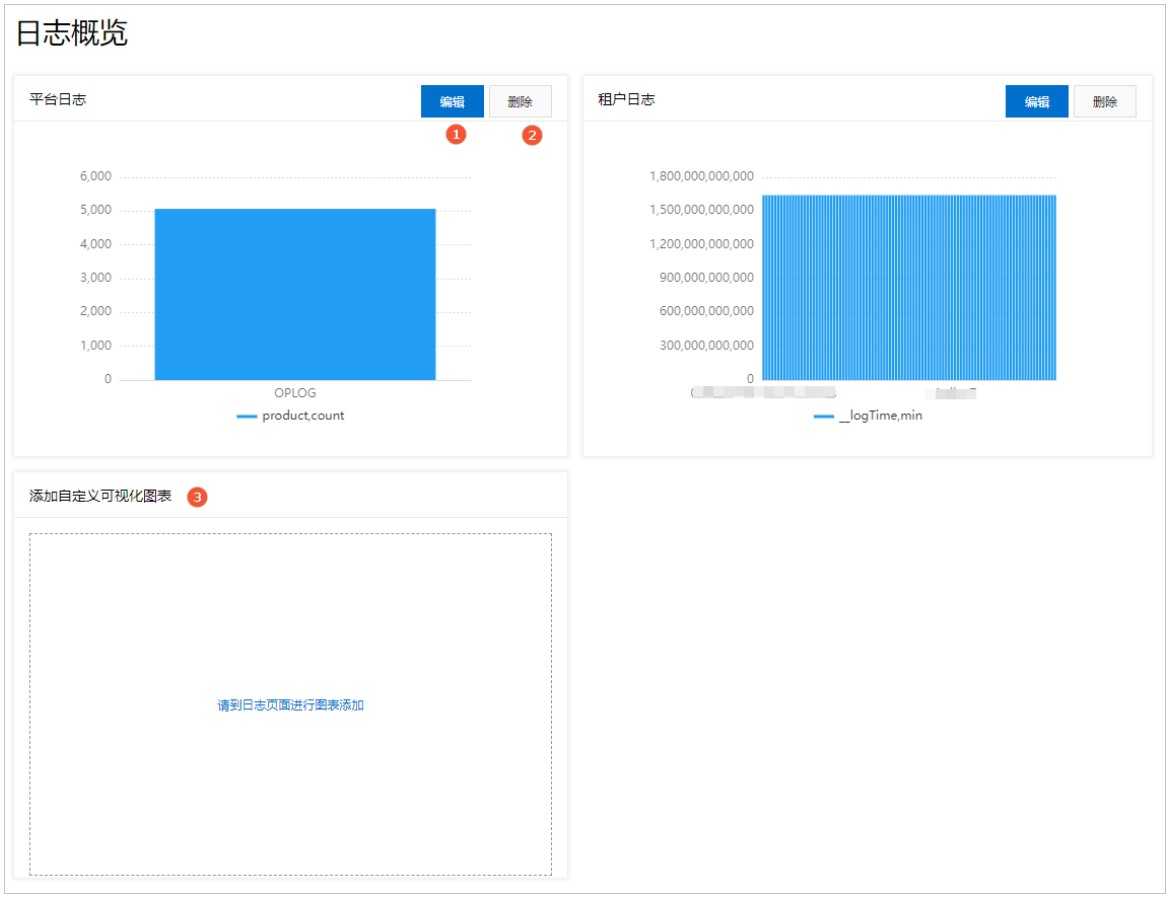
9.5.1. 查看日志概览

本文介绍如何查看各类型日志审计的可视化图表总览。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**日志管理 > 日志概览**。
4. 在**日志概览**页面，查看日志的可视化图表。

   日志概览为您展示您添加日志的可视化图表。您可以编辑或者删除日志可视化图表，也可以添加其他日志可视化图表。



- 修改可视化图表（图示①）
  a. 单击目标图表右上角的**编辑**。
  b. 在**编辑**页面，更新**图表类型**、**分类域**、**数值**。各类图表的**分类域**、**数值**设置规则如下所示：
     - **分类域**：当您设置**图表类型**为**柱状图**、**折线图**、**饼图**、**表格**时，需要设置该参数。
     - **数值**：当您设置**图表类型**为**饼图**、**单值图**时，需要设置该参数。
  c. 单击**更新**，在页面右侧预览可视化图表最新效果。



  d. 如需更新图表名称，编辑图表上方的名称。

e. 单击**确定**。**日志总览**页面会显示最新图表内容。

- 删除可视化图表（图示②）
  a. 单击目标图表右上角的**删除**。
  b. 在对话框，单击**确定**。**日志总览**页面会删除目标图表内容。
- 添加自定义可视化图表（图示③）
  a. 在**日志总览**页面最下方的**添加自定义可视化图表**区域，单击**请到日志审计页面进行图表添加**。
  b. 在**日志审计**页面添加自定义可视化图表。具体操作，请参见查看日志审计。

9.5.2. 查询原始日志

云安全管理中心提供查询原始日志功能，原始日志作为必要的调试信息，帮助安全管理员定位系统出现的故障。本文介绍如何查询原始日志。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**日志管理 > 日志查询**。
4. 在**日志查询**页面，设置查询的**时间**、**组织**、**系统类别**、**日志源**、**日志类型**以及**查询语法**，然后单击**搜索**。

   查询到的日志数量以柱状图的形式为您展示，日志详细信息以列表形式为您展现。支持查询的语法如下：

   - **全文匹配**

     示例1：12.12.12.12；示例2：www.bai*.c?m。

   - **按字段匹配查询**

     示例1：

     ```
     src_ip: 12.12.12.12 AND hostname:abc?o*al OR filesize:>100
     ```

     示例2：

     ```
     12.12.12.12 AND appName:yundun-soc
     ```

   - **类SQL查询**

     示例1：

     ```
     select * from mytable where src_ip = '12.12.12.12' order by gmt_create desc
     ```

     示例2：

     ```
     select src_ip, count(*) as cnt, max(filesize) as filesize from mytable group by src_ip limit 10
     ```

     示例3：

     ```
     select count(*) as cnt from mytable where hostname like '%abc%'
     ```

> 注意
>
> - 字段匹配查询，逻辑符AND|OR|NOT为大写字母。
> - SQL语句查询，数据库表名统一填写为mytable。
> - SQL语句查询，暂不支持常用的UDF函数和嵌套SQL语法。
> - SQL语句查询，暂不支持distinct操作。
> - SQL语句查询，支持统计函数的别名转换(count(*) as cnt)，不支持字段的别名转换(src_ip as ip)。
> - SQL语句聚合查询，仅支持String类型的字段聚合。
> - 使用通匹符查询时，如出现查询超时，可缩小查询范围再次尝试。

5. 在日志列表区域，勾选需查询的字段，查看匹配到查询字段的日志。

   您也可以展开目标展示字段，显示该字段的相同属性（字段值）计数的Top5。

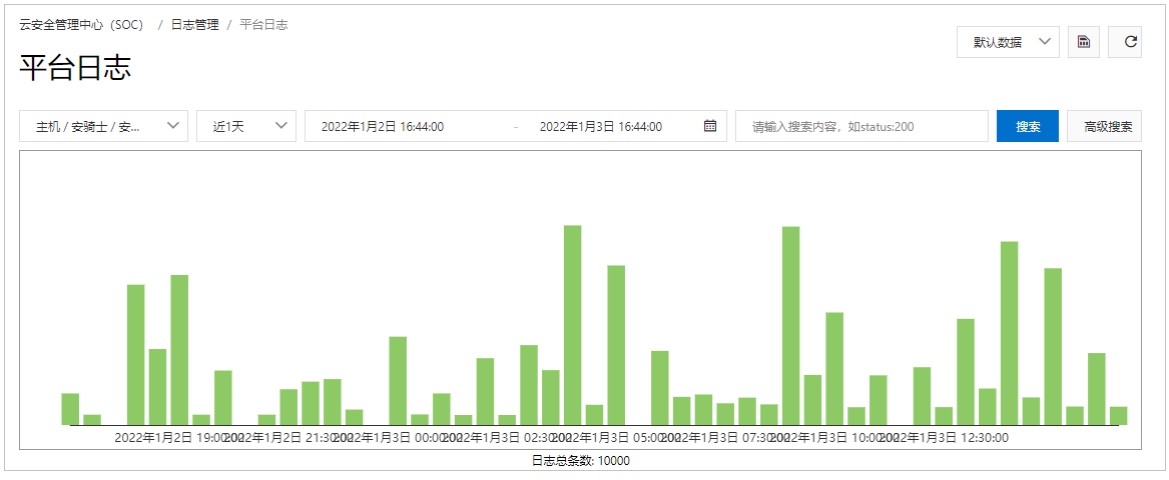
9.5.3. 查看平台日志

平台日志功能汇总平台侧的日志信息，便于安全管理员准确定位平台的问题。本文介绍如何查看平台日志。

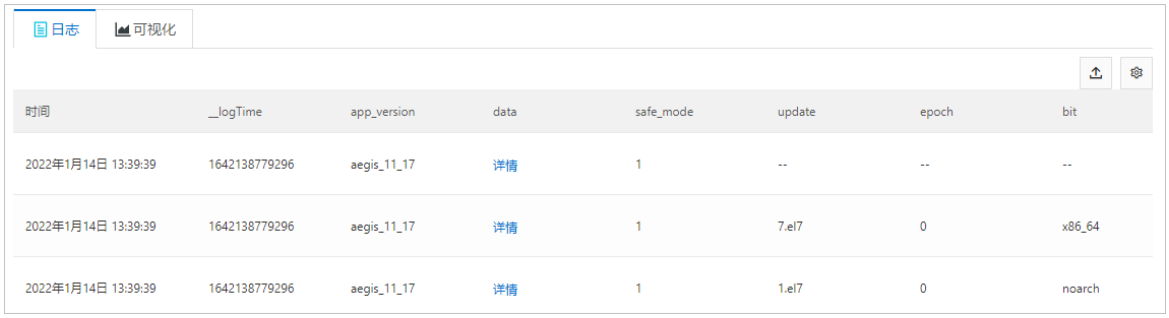
操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**日志管理 > 平台日志**。
4. 在**平台日志**页面，根据实际需要，设置数据来源、时间范围、查询内容查询。您也可以单击**高级搜索**，使用DSL语句精确查询日志。

   根据查询条件，系统会以柱状图的形式为您展示平台日志。您可以通过柱状图，了解指定时间范围内不同时间的日志数量。



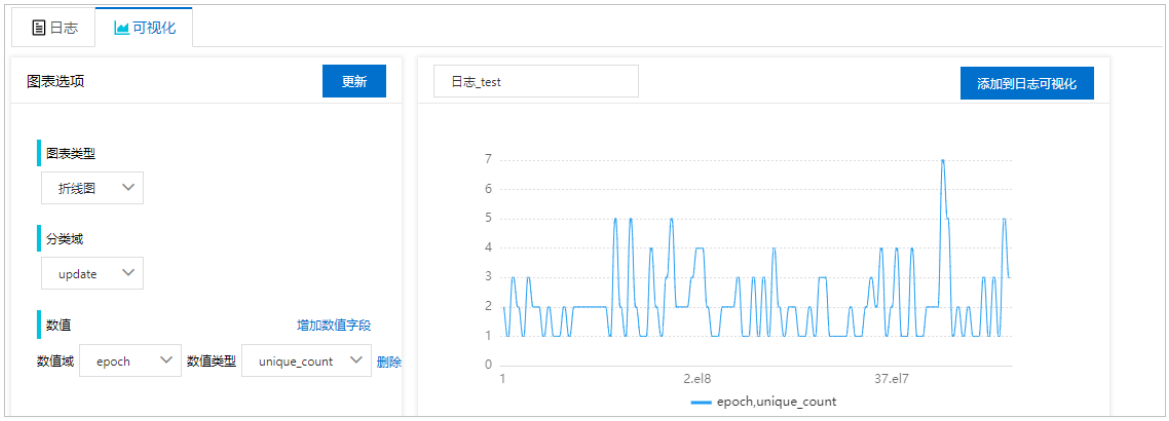
5. 在**平台日志**页面下方的**日志**页签，查看查询到的日志详细信息。



- 设置展示字段：单击 ，设置日志列表中显示的字段信息。
- 查看日志详情：单击**详情**，查看目标日志的原始日志。
- 导出日志列表：单击 ，导出查询到的日志列表。

6. 单击**可视化**，设置图表选项，查看日志的可视化图表信息。

   如果需要将日志可视化图表添加到**日志概览**页，方便您及时跟踪日志信息，请先添加日志图表的名称，然后单击**添加到日志可视化**。



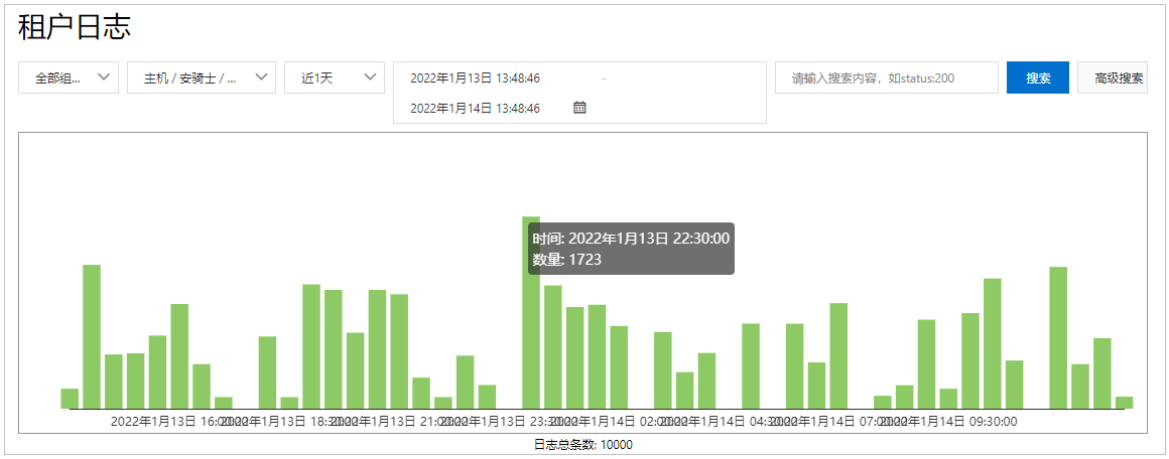
参数	说明
图表类型	**日志总览**页面中显示的日志图表类型。可选值：**柱状图**、**折线图**、**饼图**、**单值图**、**表格**。
分类域	**图表类型**选择**柱状图**、**折线图**、**饼图**、**表格**时，需要设置该参数。 可视化图表中的分类。
数值域	可视化图表中的数值分类。
数值类型	可视化图表中数值的类型，可选值：count、max、min、avg、sum、unique_count、median。 图表中需要多个数值时，单击**增加数值字段**，可设置多个**数值域**和**数值类型**。

9.5.4. 查看租户日志

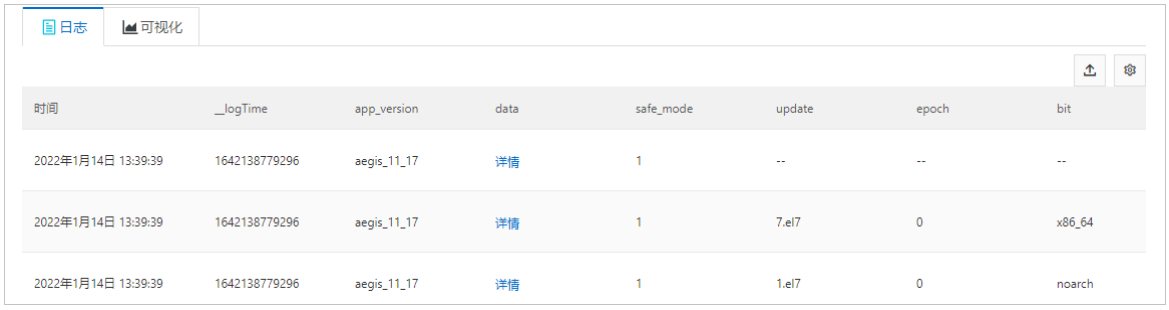
租户日志功能汇聚租户侧的日志信息，便于安全管理员定位租户侧的问题。本文介绍如何查询租户日志。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**日志管理 > 租户日志**。
4. 在**租户日志**页面，根据实际需要，设置**数据来源**、**时间范围**、查询内容。您也可以单击**高级搜索**，使用DSL语句精确查询日志。

   根据查询条件，系统会以柱状图的形式为您展示**租户日志**。您可以通过柱状图，了解指定时间范围内不同时间的日志数量。



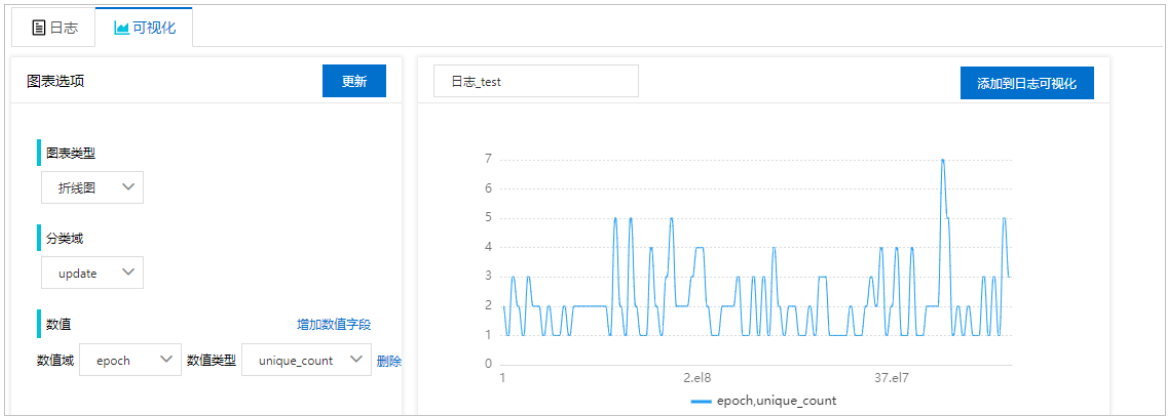
5. 在**租户日志**页面下方的**日志**页签，查看查询到的日志详细信息。



   - 设置展示字段：单击 ，设置日志列表中显示的字段信息。
   - 查看日志详情：单击**详情**，查看目标日志的原始日志。
   - 导出日志列表：单击 ，导出查询到的日志列表。

6. 单击**可视化**，设置图表选项，查看日志的可视化图表信息。

   如果需要将日志可视化图表添加到**日志概览**页，方便您及时跟踪日志信息，请先添加日志图表的名称，然后单击**添加到日志可视化**。



参数	说明
图表类型	**日志总览**页面中显示的日志图表类型。可选值：**柱状图**、**折线图**、**饼图**、**单值图**、**表格**。
分类域	**图表类型**选择**柱状图**、**折线图**、**饼图**、**表格**时，需要设置该参数。 可视化图表中的分类。
数值域	可视化图表中的数值分类。
数值类型	可视化图表中数值的类型，可选值：count、max、min、avg、sum、unique_count、median。 图表中需要多个数值时，单击**增加数值字段**，可设置多个**数值域**和**数值类型**。

9.5.5. 日志配置

9.5.5.1. 管理日志源

本文介绍如何管理SOC接入的日志源。

管理日志源

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**日志管理 > 日志配置**。
4. 在**日志配置**的**日志源管理**页签，单击**新建日志源**。
5. 在**新建日志源**面板，根据下表配置相关参数。

配置项	说明
日志源	目前只支持第三方网元。
名称	设置日志源的名称。支持0~64个字符。

配置项	说明
系统类别	设置系统类别，目前支持**主机**、**存储**、**应用**、**网络**、**数据**、**安全**及**其他**类别。
可信度	从日志源获取的日志数据可信度，此数值将作为日志关联分析的权重值，影响最终的分析结果。取值范围：0~100。
数据协议	设置数据协议。取值： ○ **Syslog** ○ **SLS**
IP地址	输入IP地址。
主机名	输入主机名。
网络协议	设置网络协议。取值： ○ **UDP** ○ **TCP**
日志解析	设置日志解析模板。 单击**新建解析模板**，新创建日志解析模板；或者选择已保存的解析模板。具体步骤，请参见设置日志解析模板。
存储时间	设置存储时长。范围：0~180天。
权限范围	设置日志的权限范围。取值： ○ **平台级** ○ **租户级** 如果您需要相关威胁告警在运营中心中呈现，请勾选对应的选项。
备注信息	输入相关说明。支持0~128个字符。

6. 单击**确定**。
日志源新建成功后，会显示在日志源列表中。您可以根据实际业务，对日志源信息重新编辑或者删除。如果日志源列表的数据较多，您可以通过页面上方**系统类别**、**数据来源**、**数据协议**、**启用状态**进行查找。



9.5.5.2. 设置日志解析模板

云安全管理中心为提供日志解析功能，安全管理员可以根据业务需要，设置日志解析模板，进而更高效地管理日志。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**日志配置**页面，单击**日志解析**。
4. 在**日志解析**页面，单击**保存解析模板**。
5. 在**保存解析模板**页面，设置**模板名称**和**适用范围**。然后单击**下一步**。
6. 单击**新建规则**，添加关联的规则信息。
   i. 设置规则信息。

      设置**规则名称**、**日志类型**。然后单击**下一步**。

      目前支持的日志类型包含：**系统日志**、**操作日志** 、**网络日志**、**威胁日志**、**应用日志**和**其他类型**的日志。

   ii. 设置日志解析方式。

      输入**日志样例**、**日志标识**并选择对应的**解析方式**。然后单击**解析**。待解析完成后，单击**下一步**。

      单击**继续解析**，可设置多个解析步骤完成原始日志的解析。

   iii. 设置日志标准化。

      设置日志标准化字段映射，然后单击**完成**。

   如果您想添加多个规则，请重复上述步骤。
7. 待规则全部添加完成后，单击**确认**。
   您保存的解析模板会显示在日志解析列表中，您可以根据实际业务编辑或者删除日志解析模板。



9.5.5.3. 设置日志转发

云安全管理中心提供日志转发功能，安全管理员可以根据业务需要，设置日志转发，方便及时查看日志信息。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**日志管理 > 日志配置**。
4. 在**日志配置**页面，单击**日志转发**。

5. 在**日志转发**页签，根据下表介绍设置配置项。

配置项	说明
日志转发	开启或者关闭日志转发开关。
IP：Port	设置日志转发的服务器或者第三方平台IP及对应端口号。 如果您需要添加多个IP及端口号，单击**继续添加**即可。
数据协议	支持的数据协议。唯一取值：Syslog。
转发日志	从**日志源**列表中，选择需要的日志源显示在**转发列表**中。

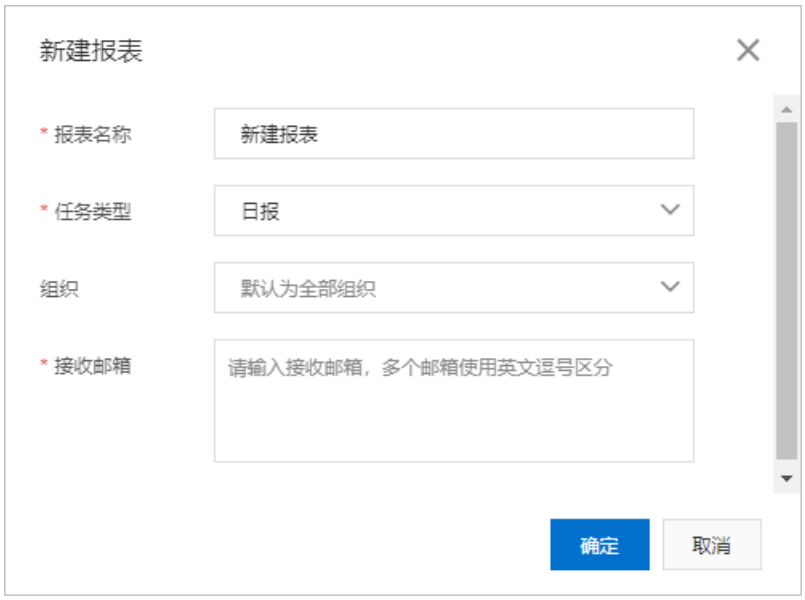
6. 单击**保存**。

9.6. 管理报表

本文介绍如何新增报表任务。新增报表任务后，系统将根据您设置的周期发送报表。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**报表管理**。
4. 在**报表管理**页面，单击**新建报表**。
5. 在**新建报表**对话框中，设置参数。



参数	说明
报表名称	设置报表任务的名称，建议使用报表用途等信息，用于后续的识别和管理。
任务类型	选择报表的类型，支持**日报**、**周报**和**月报**。

参数	说明
组织	选择报表涉及的组织。
接收邮箱	设置报表接收人的邮箱，多个邮箱使用半角逗号（,）区分。

6. 单击**确定**。

执行结果

在报表任务列表中，可以查看已经新增的报表任务信息，并执行下载、编辑、删除等操作。

9.7. 规则管理

9.7.1. 分析规则

分析规则是对众多日志数据的综合关联分析，根据检测发现的高级威胁，还原多阶段攻击的完整攻击路径。安全管理员可以简单、快速地发现高价值风险信息，提升安全运营效率。

操作步骤

云安全管理中心根据常见业务需求，为您预定义了部分规则，预定义的规则只支持查看详情，不支持修改等操作。如果预定义的规则未覆盖您的业务，您可以根据如下操作新建规则。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**规则管理 > 分析规则**。
4. 在**分析规则**页面，单击**新建规则**。
5. 在**新建规则**页面，设置如下配置项。

配置项	说明
威胁名称	设置威胁的名称。
威胁级别	设置威胁的级别。取值： ○ **信息** ○ **可疑** ○ **一般** ○ **严重** ○ **紧急**

配置项	说明
威胁类型	设置威胁的类型，可多选。取值： ○ **网络扫描** ○ **漏洞利用** ○ **恶意软件** ○ **网络攻击** ○ **风险连接** ○ **非法提取** ○ **异常行为**
ATT&CK ID	涉及的ATT&CK ID。
关联时序	设置关联时序。取值： ○ **同周期内发生**：表示在同一周期内发生的威胁事件。 ○ **顺序发生**：表示按顺序发生的威胁事件。
关联对象	设置关联的对象。目前只支持关联**同一资产**。
关联驱动条件	设置关联驱动条件。配置项如下： ○ **关联类型**：包含**必要条件**、**充分条件**。 ○ **日志范围**：包含**日志源**、**日志类型**、**日志级别**。 ○ **源IP**、**目的IP**。 ○ **关键字**：多个关键字用半角分号（;）分隔。 ○ **时间周期**：支持0~1440分钟。 ○ **日志数量**：日志的个数。 ○ **所属攻击阶段**：包含**载荷投递**、**漏洞利用**、**后门植入**、**命令控制**、**扫描扩散**、**目标打击**。
规则执行周期	设置规则执行的周期。默认为5分钟。
威胁描述	设置威胁的描述信息。支持0~256个字符。
处置建议	设置对应的处理建议。支持0~256个字符。

6. 单击**确定**。
   创建好的规则显示在规则列表中。



根据实际业务需要，您可以对自定义的规则执行**编辑**和**删除**操作。

9.7.2. 封禁规则

您可以通过一键封禁功能手动封禁风险目标。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**规则管理 > 封禁规则**。
4. 在**封禁规则**页面，单击**添加**。
5. 在**添加**对话框，设置如下配置项。

配置项	说明
IP协议	设置协议类型，可选值：**IPv4**、**IPv6**。
源IP	设置封禁的源IP地址。
目的IP	设置封禁的目的IP地址。
目的端口	设置封禁的目的IP地址端口。
禁封时长	选择封禁的时长，可选**1天**、**7天**和**30天**。
类型	设置封禁类型，可选**白名单**和**黑名单**。
备注	输入封禁原因的描述信息。

6. 单击**确定**。
创建好的封禁规则显示在规则列表中，您可以根据业务需要，执行**查询**或者**删除**操作。



9.8. 运营管理

9.8.1. 安全审计

9.8.1.1. 概述

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。

9.8.1.2. 查看审计汇总信息

本文介绍如何查看审计的汇总信息。

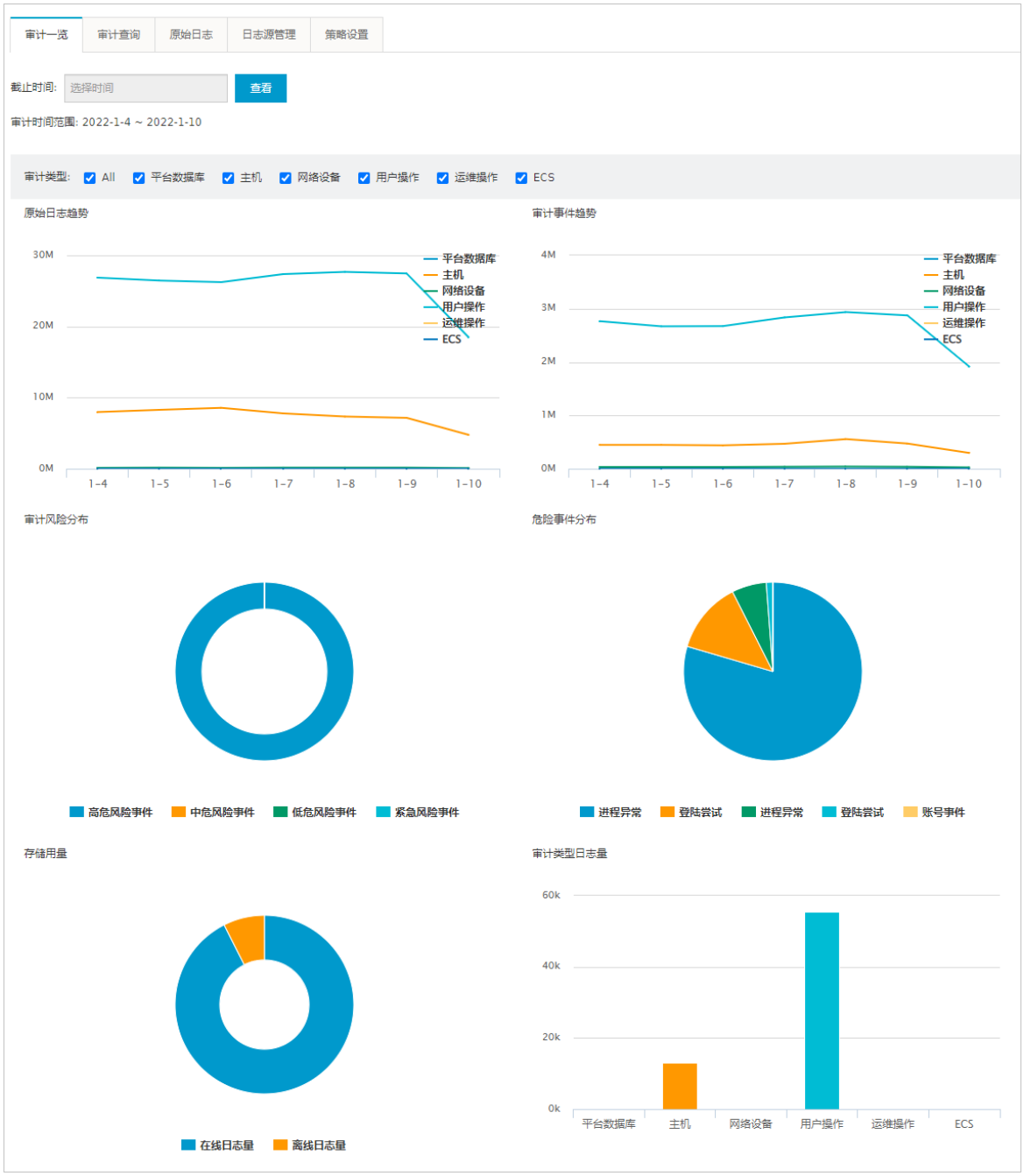
背景信息

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。

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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**审计一览**。
5. 在**审计一览**页签，查看最近7天的审计汇总信息。



- 原始日志趋势

  该模块展示**平台数据库**、**主机**、**网络设备**、**用户操作**、**运维操作**、ECS一周内产生的日志。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

  该模块展示**平台数据库**、**主机**、**网络设备**、**用户操作**、**运维操作**、ECS一周内产生的审计事件。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

  该模块展示一周内高风险、中风险、低风险事件。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

该模块展示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。

- 存储用量

  该模块展示在线日志量和离线日志量的占用情况。当存储用量过高，安全管理员需要备份清理相关审计日志。

- 审计类型日志量

  该模块展示各审计类型的日志量分布。

6. 查看指定时间段的审计汇总信息。
   i. 在**截止时间**中，选择需要查看的截止时间。
   ii. 在**审计类型**中，选中需要查看的审计类型。
   iii. 单击**查看**，可查看截止至该时间7天内的审计汇总信息。

9.8.1.3. 查询审计事件

本文介绍如何查询审计事件。

背景信息

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。

审计事件生成的过程：系统基于安全审计模块收集到的日志去匹配审计规则，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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**审计查询**。
5. 在**审计查询**页签，设置查询条件，查看该时间段内发现的审计事件。
   - 基础查询条件
     a. 设置**审计类型**、**审计对象**、**操作类型**、**操作风险级别**、**是否告警**等信息。
     b. 设置查询的时间范围。
     c. 在**全文检索**中，输入关键字信息。
     d. 单击**查询**。
   - 高级查询条件

     除基础查询条件外，还支持设置更详细的过滤条件。
     a. 设置基础查询条件。
     b. 单击**高级查询**。
     c. 在**过滤条件**中，设置**过滤名称**、**发起者**、**目标**、**命令**、**结果**、**原因**。
     d. 单击**保存过滤条件**。
6. 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，请参见管理导出任务。

9.8.1.4. 查看原始日志

本文介绍如何查看审计的原始日志。

背景信息

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. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**原始日志**。
5. 在**原始日志**页签，设置查询条件，查看该时间段内的日志统计趋势和原始日志。
   i. 设置**审计类型**和**审计对象**。
   ii. 输入查询关键字。
   iii. 设置查询时间段。
   iv. 单击**查询**。
6. 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，请参见管理导出任务。

9.8.1.5. 查看日志量

本文介绍如何查看和管理日志源。

背景信息

您可以从审计对象和设备实例两个维度查看日志量和设置是否显示日志。

- 以审计对象为维度，统计所有设备实例中包含该审计对象的日志量。
- 以设备实例为维度，统计该设备实例中所有审计对象的日志量。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**日志类型设置**，根据日志的审计对象查看日志量。

   您可以通过审计对象维度，查看该审计对象的当日日志量和30天日志量。

   在展示日志数据时，设置不显示该审计对象的日志数据，操作如下：
   i. 在审计对象的**操作**栏中，单击**不显示**。
   ii. 在提示确认框中，单击**确定**。

> **说明** 设置显示日志数据，操作方式类似。

5. 单击**日志源设置**页签，根据设备实例查看和管理日志量。

   您可以通过设备维度，查看每个实例当日日志量和30天日志量。

   在展示日志数据时，设置不显示该实例的日志数据，操作如下：

   i. 在实例的**操作**栏中，单击**不显示**。

   ii. 在提示对话框中，单击**确定**。

> **说明** 设置显示日志数据，操作方式类似。

9.8.1.6. 策略设置

9.8.1.6.1. 管理审计规则

本文介绍如何新增、修改和删除审计规则。

背景信息

当日志记录匹配审计规则时，就会上报审计事件。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，定义了默认的审计规则。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规则。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**策略设置**。
5. 在**策略设置**页签下，单击**审计规则**。
6. 新增审计规则。

   i. 单击**新增**。

ii. 在**新增规则**对话框中，设置审计规则。



iii. 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。

7. 管理审计规则。

   除了新增审计规则外，您也可以进行查询、禁用、启用、删除等操作。

   - 查询审计规则

     设置**审计类型**和**审计对象**，在输入框中输入关键字，单击**查询**。

   - 禁用审计规则

     在审计规则的**操作**栏中，单击**禁用**。

   - 启用审计规则

     对于已被禁用的审计规则，在审计规则的**操作**栏中，单击**启用**。

   - 删除审计规则

     在审计规则的**操作**栏中，单击**删除**。

     > **说明** 只能删除自定义规则，系统默认规则无法被删除。

9.8.1.6.2. 设置告警接收人

本文介绍如何设置安全审计的告警接收人。

背景信息

设置告警接收人后，在发生审计事件时，系统会将事件上报至所设置的告警接收人的邮箱中。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**策略设置**。
5. 在**策略设置**页签，单击 **告警设置**。
6. 新增告警接收人。
   i. 单击**新增**。
   ii. 在**新增报警接收人**对话框，配置告警接收人信息。



   iii. 单击**确定**。
7. 管理告警接收人。
   - 查询告警接收人

     选择**审计类型**、**审计对象**、**风险等级**，输入邮箱关键字，单击**查询**，查看当前已设置的告警接收人。
   - 删除告警接收人

     邮箱列表中，在对应邮箱的操作栏下，单击**删除**，可删除告警接收人。

9.8.1.6.3. 查询事件日志存档

本文介绍如何查询和下载审计事件和原始日志的存档。

背景信息

管理员可以下载事件和日志的存档信息到本地，进一步分析审计事件问题，保障专有云环境的安全。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**策略设置**。
5. 在**策略设置**页签下，单击**存档管理**。
6. 查询事件日志归档信息。
   i. 设置**审计类型**、**归档类型**。
   ii. 设置查询的时间段。
   iii. 单击**查询**，查询归档信息。

   在归档信息的**操作**栏，单击**下载**，可将存档文件保存到本地。

9.8.1.6.4. 下载导出的任务

本文介绍如何下载导出的审计事件或者日志。

背景信息

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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**策略设置**。
5. 在**策略设置**页签下，单击**导出管理**。
6. 查看已创建的导出任务。



7. 单击**下载**，可将导出的审计事件或日志文件下载到本地。

   如果您需要删除该任务，单击**删除**即可。

9.8.1.6.5. 修改系统配置

本文介绍如何设置安全审计的系统参数。

背景信息

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. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 安全审计**。
4. 在**安全审计**页面，单击**策略设置**。
5. 在**策略设置**页面，单击**系统设置**。
6. 在设置项的**操作**栏，单击**编辑**。



7. 填写对应的参数值，单击**确认**。

9.8.2. 配置存储策略

云安全管理中心支持您自定义日志存储策略，您可以根据业务需要，配置相关数据。本文介绍如何配置日志的存储策略。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 存储管理**。
4. 在**存储管理**页面，单击**编辑**。

   云安全管理中心会配置日志存储的默认值。如果默认值不符合您业务需要，您可以重新配置数据。

5. 在**策略管理**页签，配置日志存储、安全监控数据存储的上限、期限等信息，单击**修改**。

分类	参数	说明
日志存储（高级版）	日志存储上限	日志占用存储空间的上限阈值。
	存储最大天数	日志的存储时间周期。
安全监控数据存储（高级版）	内部RDS存储天数	安全监控数据的存储时间周期。

9.8.3. 新增自定义IP地址和地理位置

本文介绍了如何添加自定义IP地址和自定义地理位置，您可根据组网规划自定义内部IP地址，避免通用地址库的IP地址匹配到境外国家地址。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，选择**运营管理 > 全局设置 > IP地址库**。
4. 单击**添加**。

   如果需要添加多个IP地址和地理位置，可单击**批量上传（.txt文件）**将IP地址和地理位置通过模板批量导入。
5. 在**新增**对话框中，设置自定义IP地址和地理位置。



6. 单击**确定**，完成添加。
   添加完成的IP地址显示在IP地址库列表中，您可以根据业务需要，执行如下操作：
   - 修改IP地址及地理位置：

     单击目标IP地址右侧的**编辑**，在**编辑**对话框中，可修改自定义的IP地址及地理位置。
   - 删除IP地址及地理位置：

     单击目标IP地址右侧的**删除**，在**删除**对话框中，单击**确认**，即可删除自定义IP地址及地理位置。

10.可选安全产品

10.1. DDoS防护

10.1.1. 概述

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。

> **说明** DDoS流量清洗不支持专有云的内网接入交换机。

10.1.2. 查看和配置DDoS防护策略

DDoS防护内置默认的DDoS异常流量策略和DDoS清洗防御策略，您可以通过本文查看策略，并可以自定义DDoS异常流量策略。

背景信息

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设置。
- 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，能够更精准地设置对应网段的报警阈值。

操作步骤

1. 登录云盾安全中心。
2. 在控制台上方选择**安全 > 网络安全 > DDoS清洗**。
3. 在左侧导航栏选择**DDoS防护策略**，在**DDoS防护策略**页面查看和自定义DDoS异常流量策略。



操作	说明
查看默认策略	查看内置默认的异常流量策略。
自定义模式	查看和添加自定义网段的流量策略。

添加自定义网段的流量策略操作步骤如下：

i. 在**自定义模式**右侧，单击**添加**。

ii. 在**自定义异常流量阈值**对话框中，自定义网段的DDoS流量阈值。

参数	说明
网段信息	设置预警的IP网段。 **说明** 添加阈值时，务必确认已添加对应的网段，具体操作请参见添加流量采集网段。
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）

iii. 单击**确定**。

4. 在**DDoS清洗防御策略**中，单击**查看**，查看DDoS清洗防御策略。



10.1.3. 查看DDoS流量清洗事件

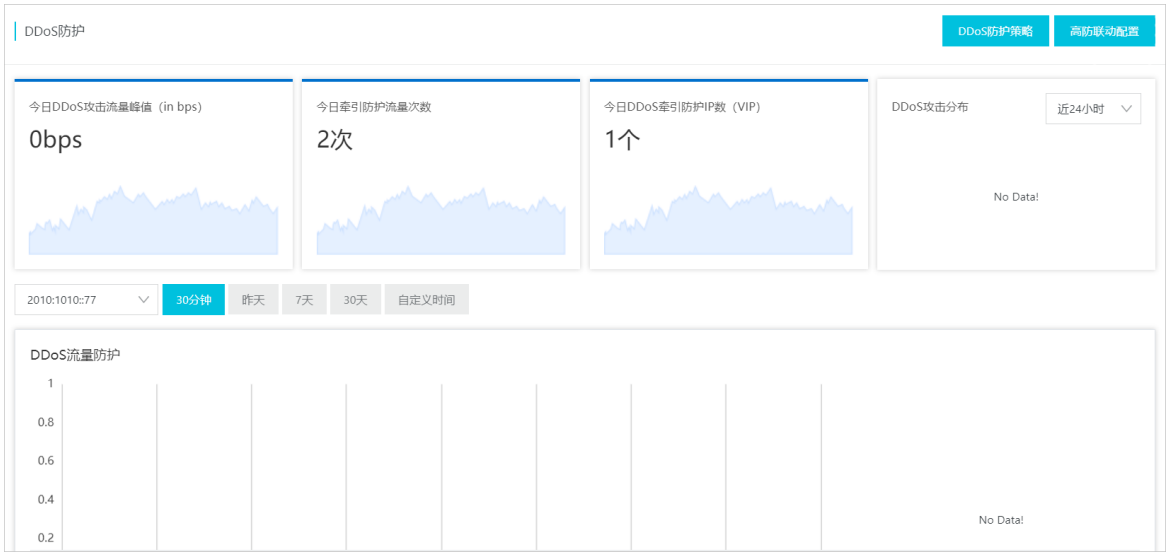
本文介绍如何查看DDoS流量清洗事件。

背景信息

云盾在流量清洗过程中或流量清洗结束时，会上报安全事件到云盾安全中心。

操作步骤

1.
2. 在控制台上方选择**安全 > 网络安全 > DDoS清洗**。
3. 在左侧导航栏选择**DDoS防护**，在**DDoS防护**页面查看DDoS防护的统计信息。



4. （可选）在**DDoS攻击清洗列表**区域，设置搜索条件，单击**搜索**，根据查询条件返回满足条件的DDoS清洗事件列表。

> **说明** 如果需要查看所有流量清洗事件，则忽略此步骤。



搜索项目	说明
IP地址	表示受到DDoS攻击的IP。
触发原因	表示DDoS攻击流量中哪一指标超过了设置的预警阈值。

搜索项目	说明
状态	DDoS攻击清洗的状态： ○ **本地清洗中** ○ **切向高防中** ○ **切回本地中** ○ **本地清洗结束** ○ **云清洗结束** ○ **云黑洞中**
起始和结束时间	DDoS清洗的起始和结束日期。

5. 在清洗事件列表中，查看DDoS流量清洗事件详情。

10.2. 云防火墙

10.2.1. 策略配置

10.2.1.1. 互联网边界防火墙同步资产

当新增的IP资产不在互联网边界防火墙的IP列表中，通过同步资产功能，系统主动更新IP列表。本文介绍如何为互联网边界防火墙手动同步资产。

1.
2. 在控制台右上方，单击**安全**，选择**网络安全 > 云防火墙**。
3. 在左侧导航栏，单击**防火墙开关策略**。
4. 单击**互联网边界防火墙**页签，在页面的右上角单击**同步资产**。
5. 在**同步资产**对话框中，单击**确定**，完成资产同步。
   进行同步资产后，系统自动更新IP列表。

10.2.1.2. 创建VPC边界防火墙

VPC边界防火墙可以检测两个VPC间的通信流量，是一种管控专有网络VPC间流量的分布式防火墙。创建并开启VPC边界防火墙后，才可以使用云防火墙分析和控制VPC间的访问流量。本文介绍了创建VPC边界防火墙开关策略。

背景信息

VPC边界防火墙只能够在已相互连接的VPC之间创建。专有网络VPC支持通过高速通道或者云企业网实现连接。

操作步骤

1.
2.
3. 在左侧导航栏，选择**网络安全 > 策略配置 > 防火墙开关策略**。

4. 在**防火墙开关 > VPC-VPC引流**页面的实例所在行，单击**创建**。



参数名称	说明
实例名	定义VPC边界防火墙的名称。该名称用于识别VPC边界防火墙实例，建议使用具有业务意义的名称，并保证名称的唯一性。 仅支持中文、英文、数字、下划线（_）、短划线（-）的格式，且不能为纯数字。
路由表	创建VPC时，系统会自动创建一张默认的路由表，用于为专有网络添加系统路由来管理专有网络的流量。VPC支持按需创建多个路由表。 在云防火墙控制台创建VPC边界防火墙时，云防火墙自动读取VPC路由表信息。高速通道支持多个路由表，因此在高速通道下创建VPC边界防火墙时可看到多个路由表，并可以选择需要防护的VPC路由表。

参数名称	说明
目标网段	在路由表下拉列表中选中某个路由时，目标网段会自动展示该路由表的默认目标网段。如果需要防护其他网段，可手动修改目标网段。 支持添加多个网段，多个网段间用英文逗号（,）隔开。
对端路由表	确认对端VPC地域和VPC实例，选择要防护的路由表。
对端目标网段	对端VPC的目标网段。
防火墙模式	○ 测试模式：此模式用于测试网段或者IP健康状态探测，确保链路正常。 ○ 正常模式：防火墙工作模式，在此模式下防火墙进行引流并对流量进行安全防护。 ○ Bypass：旁路模式，防火墙在此模式下不进行引流操作，一般当防火墙自检失败或者健康探测失败时会自动切换到旁路模式。 创建防火墙时仅支持测试模式，创建后可以将模式修改为正常模式或者旁路模式。不支持旁路模式直接切换到正常模式，正常的切换顺序为：**旁路模式 > 测试模式 > 正常模式**。 在**健康测试**区域输入本端和对端VPC内32位测试IP。
IPS防御模式	选择入侵防御模块（IPS）的工作模式，可选项： ○ 观察模式：开启观察模式后，可对恶意流量进行监控并告警。 ○ 拦截模式：开启拦截模式后，可对恶意流量进行拦截，阻断入侵活动。
IPS防御能力	选中要开启的入侵防御策略，可选项： ○ 基础规则：开启后可为资产提供基础的防护能力，包括爆破拦截、命令执行漏洞拦截、对被感染后连接C&C（命令控制）的行为进行管控。 ○ 虚拟补丁：开启后可实时防御热门的高危应用漏洞。
开启VPC边界防火墙	开启开关，则在创建VPC边界防火墙后，自动开启VPC边界防火墙开关。如果无需自动开启VPC开关，关闭该开关即可。

5. 单击**提交**。

   当VPC边界防火墙的防火墙状态变更为**已开启**，则VPC边界防火墙正式生效。

10.2.1.3. 创建IDC-VPC边界防火墙

IDC-VPC边界防火墙可以检测IDC和VPC间的通信流量，云防火墙支持对IDC-VPC边界防火墙的访问控制。本文介绍了创建IDC-VPC边界防火墙的操作详情。

操作步骤

1.
2. 在顶部菜单栏，将光标放置在**安全**上，选择**网络安全 > 云防火墙**。
3. 在**云防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**云防火墙 > 防火墙开关策略**。

5. 在**防火墙开关**页面的**IDC-VPC引流**页签右上角，单击**创建**并完成参数配置。



参数名称	说明
实例名	定义VPC边界防火墙的名称。该名称用于识别VPC边界防火墙实例，建议使用具有业务意义的名称，并保证名称的唯一性。 仅支持中文、英文、数字、下划线（_）、中划线(-)的格式，且不能为纯数字。
机房名称	选择机房名称。
VPC实例	VPC实例的ID。该实例是VPC实例的唯一标识，云防火墙自动同步您和IDC互联的VPC实例。

参数名称	说明
VPC侧路由表	创建VPC时，系统会自动创建一张默认的路由表，用于为专有网络添加系统路由来管理专有网络的流量。VPC支持按需创建多个路由表。 在云防火墙控制台创建VPC边界防火墙时，云防火墙自动读取VPC路由表信息。高速通道支持多个路由表，因此在高速通道下创建VPC边界防火墙时可看到多个路由表，并可以选择需要防护的VPC路由表。
VPC侧目标网段	在VPC侧路由表下拉列表中选中某个路由时，目标网段会自动展示该路由表的默认目标网段。如果需要防护其它网段，可手动修改目标网段。 支持添加多个网段，多个网段间用英文逗号隔开。
IDC侧物理专线（主）	您本地IDC数据中心连接到专有云时，建立的物理专线ID。 IDC机房的CE设备要和主备交换机进行物理专线连接时，随机选取一条物理专线为主。专线信息自动同步，您创建虚拟防火墙时需指定。
VBR (主)	和IDC侧物理专线（主）绑定，用来和VPC通信的VBR。和专线绑定的VBR自动同步，您创建虚拟防火墙时需指定VBR。
IDC侧物理专线（备）	您本地IDC数据中心连接到专有云时，建立的物理专线ID。 IDC机房的CE设备要和主备交换机进行物理专线连接时，不能和主物理专线相同。专线信息自动同步，您创建虚拟防火墙时需指定。
VBR (备)	和备IDC物理专线绑定，用来和VPC通信的VBR。和专线绑定的VBR自动同步，您创建虚拟防火墙时需指定。
IDC侧目标网段	对端VPC的目标网段。
防火墙模式	可选择以下防火墙模式： ○ **测试模式**：此模式用来进行测试网段或者测试IP健康探测，确保链路正常。 ○ **正常模式**：防火墙工作模式，在此模式下防火墙进行引流并对流量进行安全防护。 ○ **Bypass**：旁路模式，防火墙在此模式下不进行引流操作，一般当防火墙自检失败或者健康探测失败时会自动切换到旁路模式。 创建防火墙时仅支持**测试模式**，创建后可以进行模式修改为**正常模式**或者**旁路模式**。不支持**旁路模式**直接切换到**正常模式**，正常的切换顺序为：**旁路模式 > 测试模式 > 正常模式**。 在**健康测试**区域输入本端VPC内32位测试IP地址。
IPS防御模式	选择入侵防御模块（IPS）的工作模式，可选项： ○ **观察模式**：开启**观察模式**后，可对恶意流量进行监控并告警。 ○ **拦截模式**：开启**拦截模式**后，可对恶意流量进行拦截，阻断入侵活动。

参数名称	说明
IPS防御能力	选中要开启的入侵防御策略，可选项： ○ **基础规则**：开启后可为资产提供基础的防护能力，包括爆破拦截、命令执行漏洞拦截、以及对被感染后连接C&C（命令控制）的行为进行管控。 ○ **虚拟补丁**：开启后可实时防御热门的高危应用漏洞。
是否支持track	有以下选项： ○ **是**：表示支持track。 ○ **否**：表示不支持track。
开启VPC边界防火墙	打开开关，在创建VPC边界防火墙时自动打开VPC边界防火墙开关。如果无需自动打开VPC边界防火墙开关，请您关闭该开关。

6. 单击**提交**。

   当IDC-VPC边界防火墙的防火墙状态变更为**已开启**，则IDC-VPC边界防火墙正式生效。

> **注意** 当您的机房已部署硬件防火墙，且采用U型连接方式和主备链路工作模式时，IDC-VPC边界防火墙不支持跨机房防护。

10.2.2. 访问控制

10.2.2.1. 管理地址簿

本文介绍如何新增和管理IP地址簿、端口地址簿。通过地址簿功能，您可以保存多个IP地址段（或多个端口）。

背景信息

您可以将常用的IP和端口保存在地址簿中，方便在互联网边界防火墙中配置使用。

新增IP地址簿

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 在**访问控制**页面，单击**互联网边界防火墙**页签。
5. 单击右上角的**地址簿管理**，单击**IP地址簿**页签。
6. 单击**新建地址簿**，设置新地址簿参数。



参数	说明
地址簿类型	选择地址簿类型，支持**IP地址段**。
地址簿名称	设置地址簿的自定义名称，地址簿名称不能重复。 仅支持中文、英文、数字、下划线（_）格式，且不能为纯数字。
IP地址	设置地址簿的IP地址段，多个IP地址段使用半角逗号（,）分隔。
描述	详细描述地址簿的内容和使用场景。 仅支持长度为2~512个字符 。

7. 单击**提交**。
   新建地址簿成功后，在**IP地址簿**页签的列表中，可以查看结果。通过单击**查看**、**编辑**或**删除**，管理地址簿列表。

新增端口地址簿

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 在**访问控制**页面，单击**互联网边界防火墙**页签。
5. 单击右上角的**地址簿管理**，单击**端口地址簿**页签。
6. 单击**新建地址簿**，设置新地址簿参数。



参数	说明
地址簿名称	设置地址簿的自定义名称，地址簿名称不能重复。 仅支持中文、英文、数字、下划线（_）格式，且不能为纯数字。
端口	设置地址簿的端口范围，多个端口区间使用半角逗号（,）分隔。
描述	详细描述地址簿的内容和使用场景。 仅支持长度为2~512个字符。

7. 单击**提交**。
   新建地址簿成功后，在**端口地址簿**页签的列表中，可以查看结果。通过单击**查看**、**编辑**或**删除**，管理地址簿列表。

10.2.2.2. 配置互联网边界防火墙

访问控制功能支持对互联网边界防火墙进行访问控制。您可在互联网边界防火墙中配置访问控制策略，限制主机对内、外双向的未授权访问。

背景信息

互联网边界防火墙支持**内对外**（用户内网访问外部互联网）和**外对内**（外部互联网访问用户的内部网络）流量的访问控制。

本文中涉及到的IP地址簿、端口地址簿和域名地址簿，如何新建请参见管理地址簿。

操作步骤

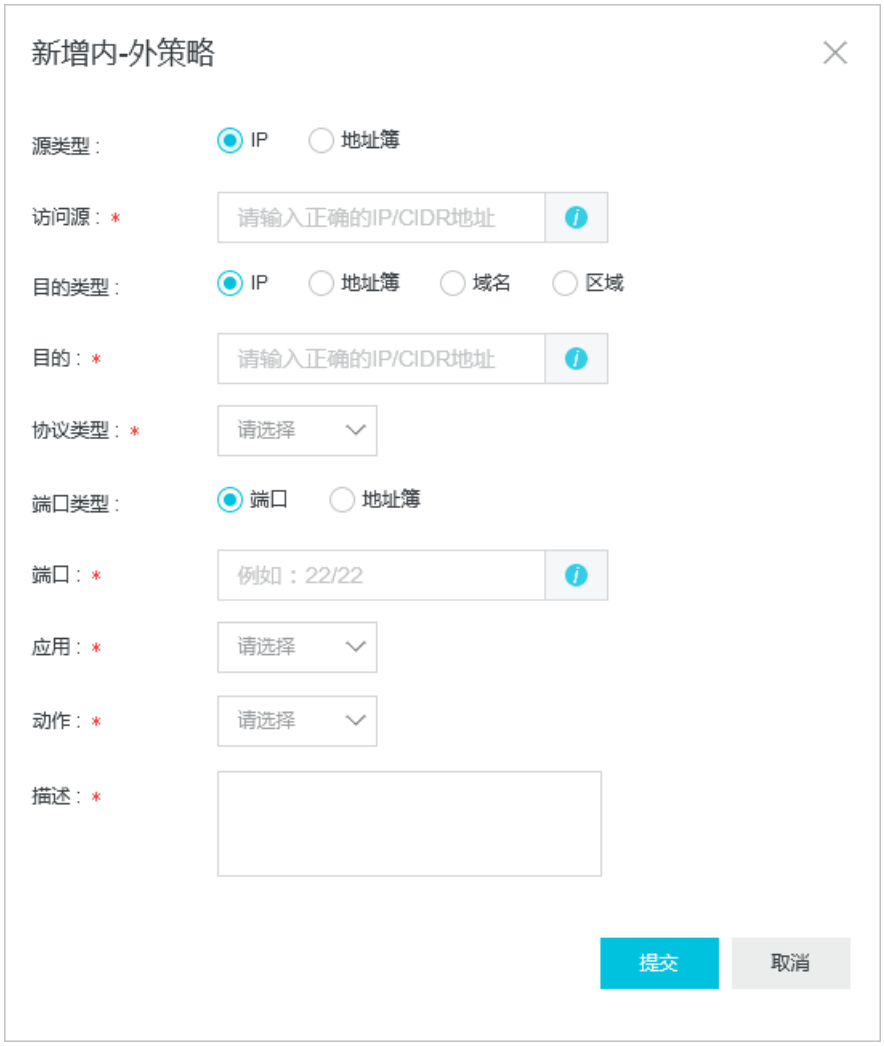
1.
2. 在控制台右上方，单击**安全**，选择**网络安全 > 云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 单击**互联网边界防火墙**页签。
5. 单击**内对外**（或者**外对内**）页签，选择网络流量方向。



- **内对外**：用户内网访问外部互联网。
- **外对内**：外部互联网访问用户的内部网络。

6. 单击**新增策略**，设置防火墙策略。

   设置**新增内-外策略**。



策略参数	配置说明
源类型	设置访问来源的类型，可选择**IP**或**地址簿**。 • **IP**：仅支持单个IP地址段。 • **地址簿**：预先配置的IP地址簿，是多个IP地址段的组合，便于您在策略配置时对多个IP地址进行限制。

策略参数	配置说明
访问源	设置访问流量的来源地址。本操作步骤中访问源代表允许访问外部互联网的IP地址。 ○ **源类型**选择**IP**时，该访问源需要设置成网段，如：1.XX.XX.1/32。 ○ **源类型**选择**地址簿**时，您可单击**从地址簿中选择**，在**IP地址簿**中选择访问源。
目的类型	设置访问目的地址的类型，可选择**IP**、**地址簿**、**域名**或**区域**。
目的	设置接收流量的目的地址。本操作步骤中**目的**代表允许访问的外部互联网地址。 ○ **目的类型**选择**IP**时，该目的需要设置成网段，例如：1.XX.XX.1/32。 ○ **目的类型**选择**地址簿**时，您可单击**从地址簿中选择**，在**IP地址簿**中选择目的地址。 ○ **目的类型**选择**域名**时，该目的需要设置成域名地址，例如：www.example.com。 ○ **目的类型**选择**区域**时，您可在下拉菜单中选择访问目的区域。
协议类型	设置该内到外访问流量的协议类型，可选择**TCP**、**UDP**、**ICMP**或**ANY**。不确定具体协议类型时可选择ANY。
端口类型	设置协议的端口类型，可选择**端口**或**地址簿**。 ○ **端口**：仅支持一个端口范围。 ○ **地址簿**：预先配置的端口地址簿，是多个端口的组合，便于您在策略配置时对多个端口进行限制。
端口	设置需要放开或限制的端口。可根据端口类型的配置项，手动输入单个端口号，或者单击从地址簿中选择，选择预先配置的端口地址簿。 ○ **端口类型**选择**端口**时，手动输入端口范围。 ○ **端口类型**选择**地址簿**时，您可单击**从地址簿中选择**，在**端口地址簿**中选择端口。
应用	设置该内到外访问流量的应用类型。
动作	设置允许或拒绝该流量通过互联网边界防火墙。 ○ **放行**：如果流量符合该策略，则直接放行该流量。 ○ **观察**：如果流量符合该策略，则记录并放行该流量。 ○ **拒绝**：如果流量符合该策略，则直接丢弃该流量。
描述	输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。 输入字符需要符合以下四类：中文、数字、字母、下划线（_）。

7. 单击**提交**，完成创建策略操作。

执行结果

创建成功后，新建的策略将在策略列表中显示。您可以在**操作**栏中对策略进行**编辑**、**删除**、**插入**和**移动**等操作。

10.2.2.3. 新增策略组

本文介绍如何在主机边界防火墙中新增策略组。您可在云防火墙中配置访问控制策略，限制ECS实例间的未授权访问。

背景信息

主机边界防火墙使用了安全组的能力，您在此页面配置的访问控制策略会自动同步到ECS安全组中。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 在**访问控制**页面，单击**主机边界防火墙**页签。
5. 单击右上角的**新增策略组**。
6. 在**新建策略组**对话框中，配置策略组。

参数	配置项描述	配置方法
策略组名称	策略组的自定义名称。字符长度限制范围为2~128。	手动输入策略组名称，便于您后续识别该策略组。
所属VPC	该策略组应用的VPC网络。	单击**所属VPC**下拉框并选择该策略组应用的VPC。 **说明** 您只可选择一个所属VPC。
实例ID	该所属VPC网络下的实例ID。	单击**实例ID**下拉框并选择该VPC网络下的实例IP。 **说明** 实例ID支持多选。
描述	该策略组的备注信息。字符长度限制范围为2~256。	手动输入描述内容，便于您后续识别该策略组。
模板	该策略组允许或拒绝流量通过的模板。	单击**模板**下拉框并选择模板类型。模板类型可选： ○ **default-accept-login**：默认放行入方向所有流量的22和3389端口。 ○ **default-drop-all**：默认拒绝该策略组中的所有流量。 ○ **default-accept-all**：默认放行该策略组中的所有流量。

7. 单击**提交**，完成策略组的创建。

10.2.2.4. 配置主机边界防火墙访问控制策略

本文介绍如何查看主机边界防火墙的策略组，配置策略组中的访问控制策略，并发布到ECS的安全组中。

背景信息

在**主机边界防火墙**页面，您可以查看自定义的策略组和从ECS同步过来的安全组。

创建自定义策略组的具体操作，请参见新增策略组。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 在**访问控制**页面，单击**主机边界防火墙**页签。
5. （可选）配置策略组过滤条件，单击**搜索**，搜索目标策略组。

   > **说明** 如果您需要查看所有策略组，可以忽略此步骤。

   在策略组列表中，您可以查看搜索结果。
6. 定位到目标策略组，配置访问控制策略。
   i. 单击**操作**列中的**配置策略**。
   ii. 在**策略配置**页面，单击**新建策略**。



> **说明** 您如果需要修改或删除访问控制策略，单击**入方向**和**出方向**页签，并单击**编辑**或**删除**按钮。

   iii. 在**新建策略组策略**对话框中，设置策略参数。



参数	说明
网卡类型	该策略应用的网络类型。 系统默认配置为**内网**表示内网间的访问流量。
策略方向	该策略控制的流量方向。可选项： ■ **入方向**：从其它ECS访问本机。 ■ **出方向**：从本机访问其它ECS。
策略类型	允许或拒绝该流量通过主机防火墙。可选项： ■ **允许**：允许该内网间流量通过。 ■ **拒绝**：不允许该内网间流量通过。
协议类型	该访问流量的协议类型。单击**协议类型**下拉框并选择对应的类型。可选项： ■ TCP ■ UDP ■ ICMP ■ ANY：表示任何协议类型。不确定该访问流量的类型时可选择ANY。

参数	说明
端口范围	该策略限制或放行某个访问流量所经过的目的端口。 手动输入端口的地址范围。例如：22/22。
优先级	该策略生效的优先级。 **说明** 主机访问控制策略优先级范围为1~100，优先级可重复。策略优先级相同时，**拒绝**策略优先生效。优先级相同的策略，如果都是**放行**类型，那这两条策略将同时生效。
源类型	该策略限制的访问源的类型。可选项： ■ **地址段访问**：该策略的访问源为地址段。 ■ **策略组**：该策略的访问源类型为策略组访问，表示访问源为该策略组中的多个实例地址。 **说明** 在ECS安全组中创建的策略，您将无法选择**策略组**作为源类型，**只允许**选择**地址段访问**源类型。
源对象	该策略访问源地址，为单个地址段或者策略组中的多个实例地址。 根据选择的**源类型**配置源对象。 ■ 源类型选择**地址段访问**时，需手动输入访问源地址段。仅支持单个地址段。 ■ 源类型选择**策略组**时，单击**源对象**下拉框并选择策略组，表示访问源为策略组中的多个实例地址。 **说明** 只允许选择单个策略组作为**源对象**。
目的选择	表示访问流量的目的地址。可选项： ■ **全部ECS**：该策略将应用到您的所有ECS中。 ■ **地址段访问**：手动输入IP、ICDR地址段。策略将应用到该地址接收的流量中。
描述	该策略的备注信息，用于区分策略的目的。 字符范围为2~256个字符。

iv. 单击**提交**，完成访问控制策略配置。

7. 在**主机边界防火墙**页签定位到目标策略组，单击**操作**列中的**发布**，使策略生效并同步到ECS安全组。

10.2.2.5. 配置VPC边界防火墙访问控制策略

云防火墙的VPC边界防火墙支持检测和控制两个VPC间的通信流量。本文介绍了VPC边界防火墙的访问控制操作。

前提条件

VPC边界防火墙默认不存在。因此在创建VPC访问控制策略前，需先创建并开启相应的VPC边界防火墙，具体操作，请参见创建VPC边界防火墙。

背景信息

VPC边界防火墙开关开启后，访问控制策略才能生效。

VPC边界防火墙默认放行所有流量，您在对VPC间流量进行管控时，需要对不可信的流量进行拒绝；或者先对可信源进行放通，再拒绝其他任意地址的访问。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**网络安全 > 云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 单击**VPC边界防火墙**页签。
5. 单击**新增策略**。
6. 在**新增VPC边界防火墙策略**中，配置访问控制策略。



参数	说明
源类型	访问源地址的类型，可选择IP或地址簿类型。 ○ **IP地址**：访问源地址类型为IP地址，需手动输入IP地址段。 ○ **地址簿**：访问源设置需从您预先配置的址簿中选择。 您可以将多个IP设置成一个地址簿，方便您在配置访问控制规则时简化规则配置。
访问源	发送流量的IP、CIDR地址。 **说明** 访问源只支持配置一个网段，例如：1.*.*.1/32。 如果源类型选择的是地址簿，需要从地址簿列表中选择一个地址簿作为访问源。
目的类型	访问目的的类型。可选值： ○ **IP地址**：访问目的设置为IP地址。 ○ **地址簿**：访问目的从地址簿中选择一组IP地址。 ○ **域名**：访问目的设置为某一个域名。域名配置支持泛域名，例如：*.aliyun.com。 **说明** 对于HTTP Header中没有Host字段或HTTPS请求没有SNI的流量默认放行。
目的	访问目的需要设置为网段；只可配置一个网段。 如果目的类型选择的是域名，可以配置为域名或泛域名，例如：*.aliyun.com。
协议类型	该访问流量的协议类型。可选值： ○ **ANY**：任何协议。 ○ **TCP**：TCP协议。 ○ **UDP**：UDP协议。 ○ **ICMP**：ICMP协议。
端口	支持配置端口范围；0/0代表任意端口。 **说明** 协议选择为ICMP，目的端口配置不生效。协议选择为ANY，对于ICMP流量做访问控制，目的端口配置不生效。

参数	说明
应用	当前支持配置的应用有： ANY、HTTP、HTTPS、Memcache、MQTT、MySQL、RDP、Redis、SMTP、SMTPS、SSH和VNC。 协议选择TCP时，支持配置不同的应用类型；如选择其他类型协议，应用类型只能设置为ANY。 **说明** 识别应用依赖应用报文的特征（协议识别不依据端口）；应用识别失败时，该会话流量会被放行。
动作	允许或拒绝该流量通过互联网边界防火墙。 ○ **放行**：允许访问。 ○ **拒绝**：禁止访问，并且不会提供任何形式的通知信息。 ○ **观察**：设置为观察模式后仍允许源到目的的访问。观察一段时间后可根据需要调整为放行或拒绝。
描述	对访问控制策略进行描述或备注。输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。

7. 单击**提交**，完成访问控制策略配置。

10.2.2.6. 配置IDC-VPC边界防火墙访问控制策略

云防火墙支持对IDC和VPC间的通信流量进行检测和访问控制。本文介绍了创建和管理IDC-VPC边界防火墙访问策略的具体操作。

前提条件

IDC-VPC边界防火墙默认不存在。因此在创建IDC-VPC访问控制策略前，需先创建并开启相应的IDC-VPC边界防火墙。

IDC-VPC边界防火墙开关开启后，访问控制策略才能生效。

背景信息

IDC-VPC边界防火墙默认放行所有流量，您在对IDC-VPC间流量进行管控时，需要对不可信的流量进行拒绝；或者先对可信源进行放通，再拒绝其他任意地址的访问。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**访问控制**。
4. 在**访问控制**页面，单击**IDC-VPC边界防火墙**页签。
5. 单击**新增策略**。
6. 在**新增VPC边界防火墙策略**对话框中，配置访问控制策略。



参数	说明
源类型	访问源地址的类型，可选值： ○ **IP**：访问源地址类型为IP地址，需手动输入IP地址段、CIDR地址。 ○ **地址簿**：访问源设置需从您预先配置的地址簿中选择。 您可以将多个IP设置成一个地址簿，方便您在配置访问控制规则时简化规则配置。
访问源	出方向策略，访问源必须是私网IP，输入格式需采用标准掩码格式，如：10.XX.XX.0/24，172.16.XX.XX/32。 如果源类型选择的是地址簿，需要从地址簿列表中选择一个地址簿作为访问源。
目的类型	可选值： ○ **IP**：访问目的设置为IP地址。 ○ **地址簿**：访问目的是从地址簿中选择的一组IP地址。 ○ **域名**：访问目的设置为某一个域名。域名配置支持泛域名，例如：*.aliyun.com。 **说明** 对于HTTP Header中没有Host字段或HTTPS请求没有SNI的流量默认放行。

参数	说明
目的	入方向策略，目的必须是私网IP，输入格式需采用标准掩码格式，如：10.1.XX.XX/24，172.16.XX.XX/32。 如果目的类型选择的是域名，可以配置为域名或泛域名，例如：*.aliyun.com。
协议类型	可选值： ○ **ANY**：任何协议。 ○ **TCP**：TCP协议。 ○ **UDP**：UDP协议。 ○ **ICMP**：ICMP协议。
端口	支持配置端口范围；0/0代表任意端口。 **说明** 协议选择为ICMP，目的端口配置不生效。协议选择为ANY，对于ICMP流量做访问控制，目的端口配置不生效。
应用	当前支持配置的应用有： ANY、HTTP、HTTPS、Memcache、MongoDB、MQTT、MySQL、RDP、Redis、SMTP、SMTPS、SSH、SSL和VNC。 协议选择TCP时，支持配置不同的应用类型；如选择其他类型协议，应用类型只能设置为ANY。 **说明** 识别应用依赖应用报文的特征（协议识别不依据端口）；应用识别失败时，该会话流量会被放行。
动作	允许或拒绝该流量通过IDC-VPC边界防火墙。可选值： ○ **放行**：允许访问。 ○ **拒绝**：禁止访问，并且不会提供任何形式的通知信息。 ○ **观察**：设置为观察模式后仍允许源到目的的访问。观察一段时间后可根据需要调整为放行或拒绝。
描述	对访问控制策略进行描述或备注。输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。

7. 单击**提交**，完成访问控制策略配置。

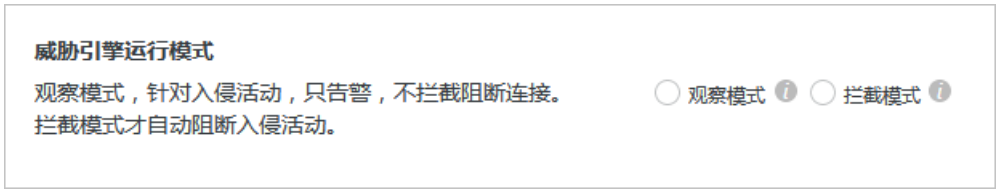
10.2.3. 入侵防御

10.2.3.1. 配置入侵防御策略

入侵防护内置了威胁检测引擎，可对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截，并提供精准的威胁检测虚拟补丁，智能阻断入侵风险。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**网络安全 > 云防火墙**。
3. 在**云防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**云防火墙 > 入侵防御策略**。
5. 在**入侵防御**页面，设置入侵防护的威胁引擎运行模式。



入侵防护支持以下两种模式：

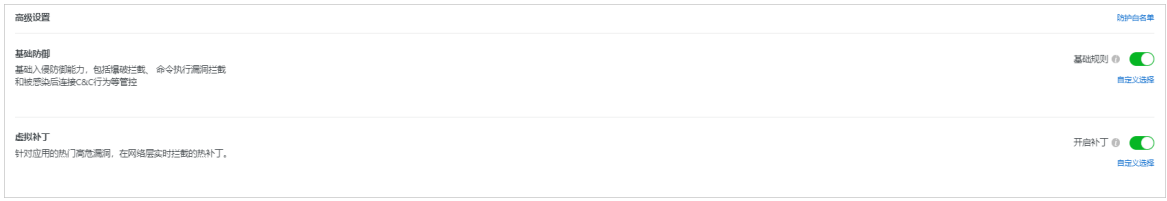
- **观察模式**：针对入侵活动，只警告，不进行拦截。
- **拦截模式**：针对入侵活动，进行拦截并警告。

以设置**拦截模式**为例，操作步骤如下：

i. 单击选择**拦截模式**。

ii. 在确认提示框中，单击**确定**。

6. 设置入侵防护的高级功能。



- 防护白名单：设置防护白名单后，云防火墙入侵防御功能将对白名单中的流量地址放行。

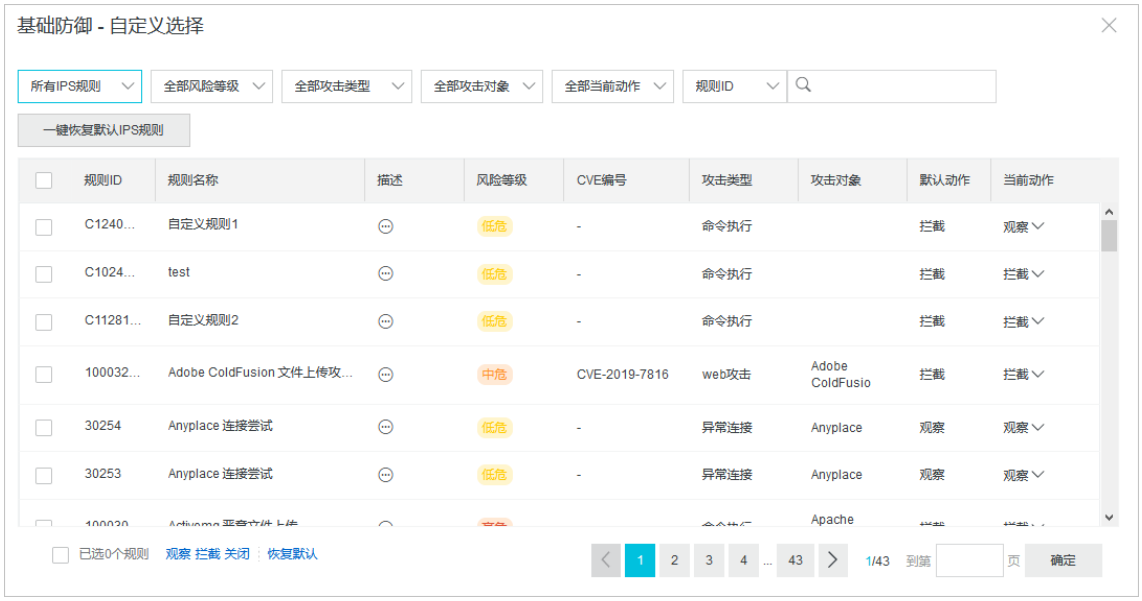
  在**高级设置**区域，单击**防护白名单**，将确定为可信的流量添加到白名单中。

  可将内外双向流量的可信源IP地址、目的IP地址或地址簿配置到防护白名单中。



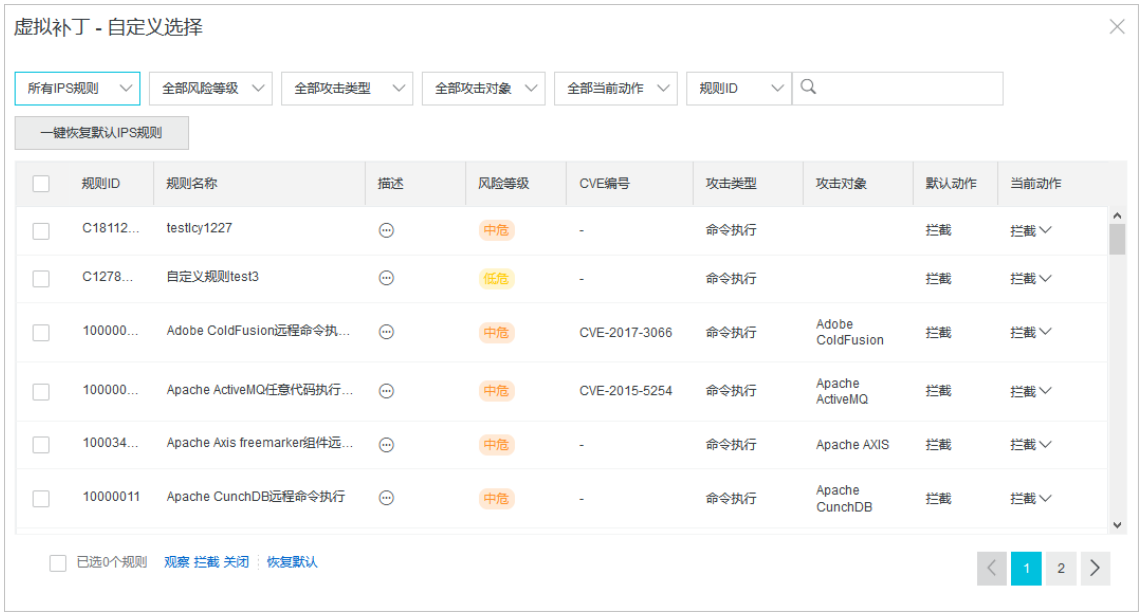
- 基础防御：可提供基础的入侵防御能力，包括爆破拦截、命令执行漏洞拦截、以及对被感染后连接C&C（命令控制）的行为进行管控。开启后可为您的资产提供基础的防护能力。

在**基础防御**区域，打开**基础规则**开关，云防火墙默认为您开启部分常见威胁相关的检测规则。如果默认规则无法满足您的需求，您可以在**基础防御**区域，单击右侧的**自定义选择**，打开**基础防御-自定义选择**对话框，对单个或多个基础防御规则进行自定义设置。自定义设置仅支持修改该基础防御规则的放行状态，即观察、拦截、关闭。



- 虚拟补丁：无需在系统上进行安装，开启后可实时防护热门的应用高危漏洞。

  在**虚拟补丁**区域，打开**开启补丁**开关，云防火墙可为您实时防护热门的高危漏洞和应急漏洞。您也可以在**虚拟补丁**区域，单击右侧的**自定义选择**，打开**虚拟补丁-自定义选择**对话框，可对单个或部分基础虚拟补丁规则进行自定义设置。



10.2.3.2. 查看IPS拦截记录

本文介绍了如何查看被云防火墙IPS功能拦截的互联网和VPC攻击的详细信息。

操作步骤

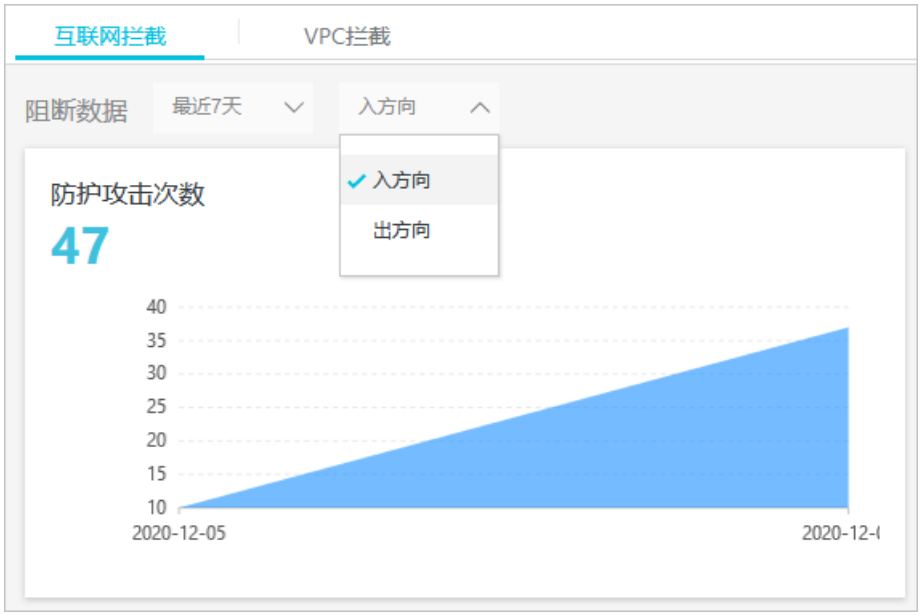
1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，选择**网络安全 > 云防火墙**。
3. 在左侧导航栏，单击**入侵防御**。
4. 在**互联网拦截**、**VPC拦截**页签，查看拦截数据的详细信息。

   信息说明如下所示：

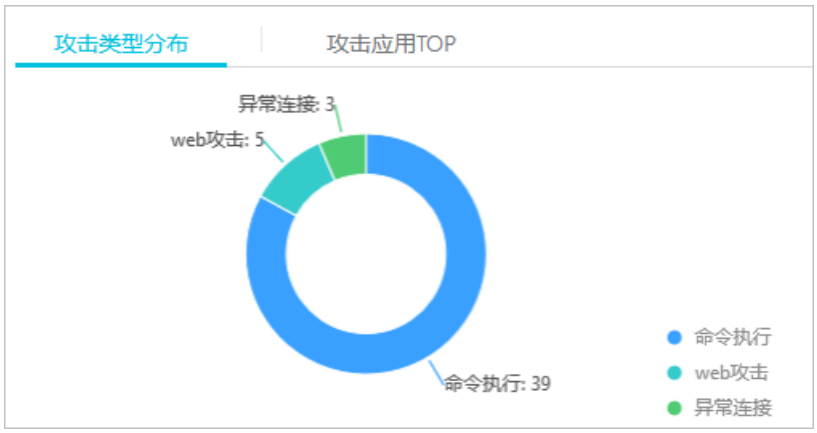
   - **互联网拦截**

     在**互联网拦截**页面，您可查看最近1小时、1天或7天内出方向或入方向的拦截活动情况。

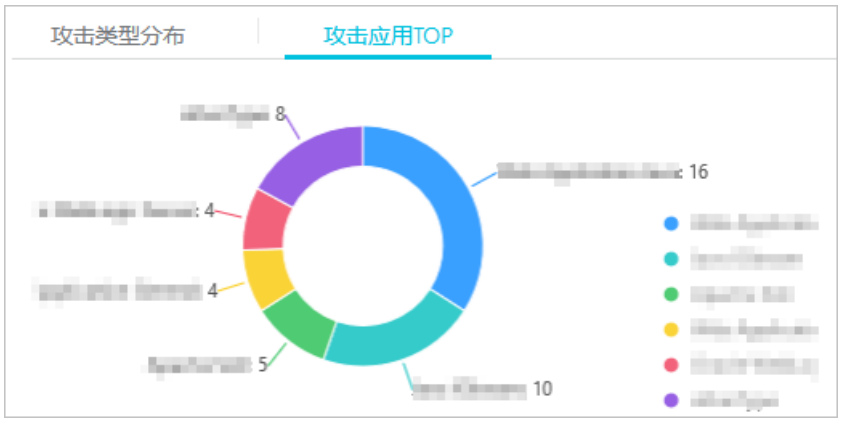


     互联网拦截页面具体包含以下模块：

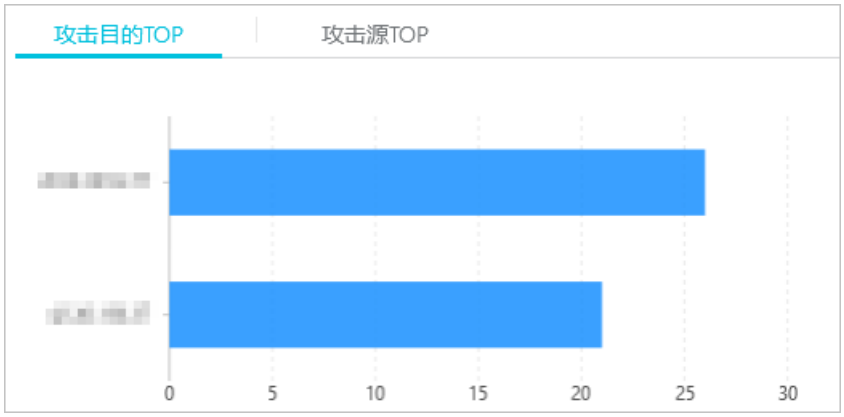
     - **防护攻击次数**：展示了被云防火墙IPS功能阻断的出方向或入方向流量的攻击次数及分布图。
     - **攻击类型分布**：展示了被云防火墙IPS功能阻断出方向或入方向流量的攻击类型分布。



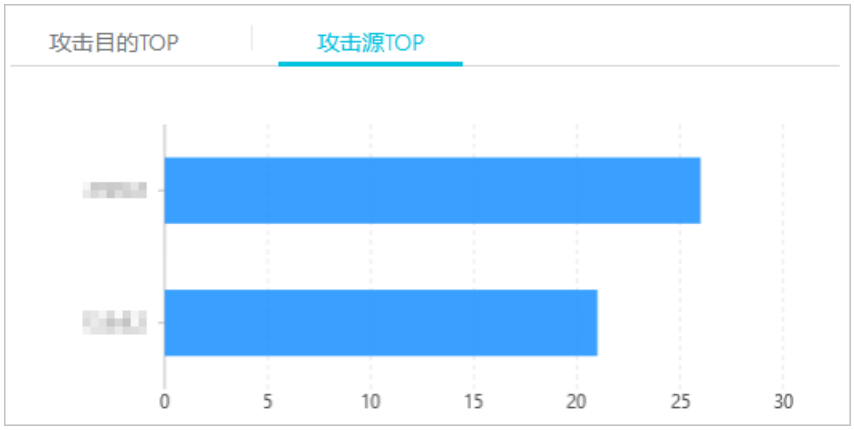
- **攻击应用TOP**：展示了被云防火墙IPS功能阻断出方向或入方向流量的应用分布。



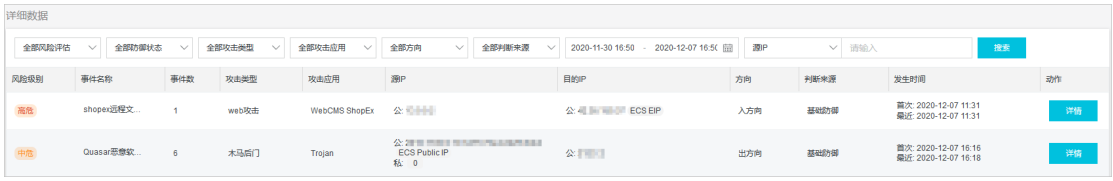
- **攻击目的TOP**：展示了被云防火墙IPS功能阻断出方向或入方向流量的攻击目的地址的流量分布。



- **攻击源TOP**：展示了被云防火墙IPS功能阻断出方向或入方向流量的攻击源地址的流量分布。



- **详细数据**：展示了所有阻断事件的详细信息，包括事件的风险级别、事件数量、源IP地址和目的IP地址等信息。



在**详细数据**模块，您可根据需要执行以下操作：

- 在搜索栏通过筛选风险级别、判断来源、方向和时间范围等定位到具体事件。
- 单击**动作**栏的**详情**可打开阻断事件的详情面板，查看事件描述等详细信息。



- **VPC拦截**

VPC拦截页面展示了云防火墙拦截到的VPC网络之间的异常事件信息。您可以查看指定时间段内VPC拦截事件的名称、风险级别、攻击类型等详细信息。



在**VPC拦截**页签，您可根据需要执行以下操作：

- 选择风险级别、防御状态、攻击类型和时间等条件后，单击**搜索**，查看符合设定条件的事件信息。

- 定位到目标事件，单击**动作**栏下的**详情**，查看当前事件的**事件描述**、**防御状态**等详细信息。

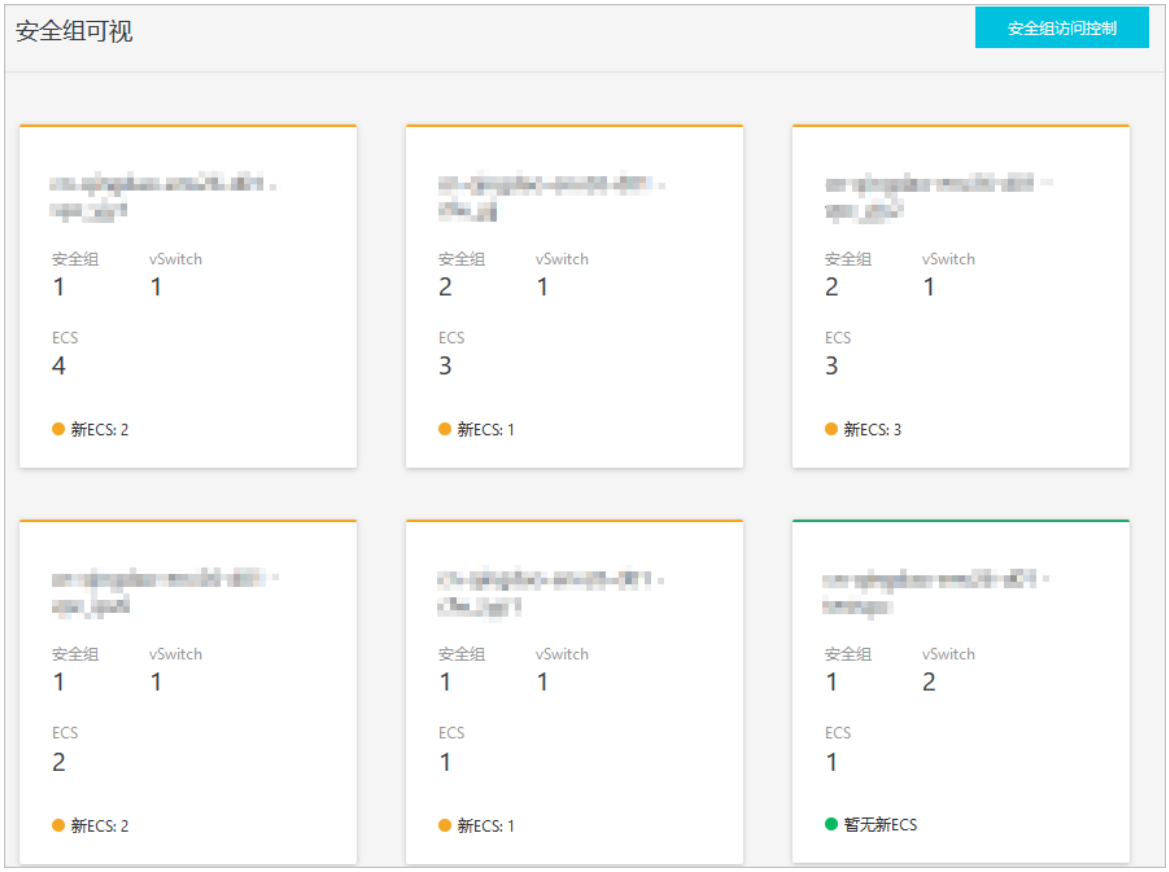


10.2.4. 查看安全组

本文介绍了如何查看VPC中安全组及ECS的详细信息及访问关系。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**安全组**。
4. 在**安全组可视**页面，查看VPC中安全组和ECS的概要信息。

   定位到需要查看的VPC区域，查看VPC中安全组、vSwitch（虚拟交换机）、ECS的总数。



5. 单击需要查看的安全组所在VPC，查看VPC中安全组和ECS的详细信息。

   可查看最近1小时、1天、7天或1个月安全组、ECS的详细信息，如下所示：

   - 查看VPC中所有安全组、ECS信息。可查看如下信息：
     - 在**安全组可视**页面右侧的**安全组视角**区域，查看VPC中安全组总数、ECS总数、首次流量次数和安全组列表。

       > **说明** 首次流量是指安全组中有依赖关系的ECS间首次产生访问流量的总次数。

       在**安全组可视**页面的面板中，默认显示所有安全组图标。在安全组列表，单击安全组**操作**列的 图标，可以隐藏面板中对应的安全组图标。

- 单击**安全组可视**页面右上角的**数据详情**，在**业务节点**页签的**安全组视角**列表查看VPC中所有安全组信息。



- 查看单个安全组及其ECS信息。可查看如下信息：
  - 在**安全组可视**页面的安全组列表，单击安全组**操作**列的 图标。在**业务节点**页签的**ECS视角**列表，查看安全组中ECS的详细信息。



- 在**安全组可视**页面的面板中，单击安全组图标。在页面右侧的**安全组视角**区域，可以查看安全组中ECS总数、依赖的安全组个数、被依赖的安全组个数、首次流量次数、依赖及被依赖安全组列表。



在安全组的**数据详情**提示框中展示ECS总数、依赖及被依赖安全组个数、首次流量次数，并可查看详细信息如下所示：

- ECS详情：单击图标，查看安全组中ECS详细信息。
- 依赖安全组详情：单击图标，查看依赖安全组详细信息。
- 被依赖安全组详情：单击图标，查看被依赖安全组详细信息。
- 首次流量详情：单击图标，查看有访问关系的安全组或ECS的详细信息。

- 查看单个ECS信息。可查看如下信息：
  - 在**安全组可视**页面的面板中，双击安全组图标，面板中显示安全组中所有ECS。在页面右侧的**ECS视角**区域，可以查看安全组中ECS总数、依赖及被依赖的安全组个数、首次流量次数及ECS列表。



面板中默认显示安全组所有ECS图标。在ECS列表，单击ECS**操作**列的图标，可以隐藏面板中对应的ECS图标。

- 在**安全组可视**页面的面板中，单击ECS图标。在页面右侧的**ECS视角**区域，可以查看依赖及被依赖的ECS个数、首次流量次数、依赖及被依赖ECS列表。



在ECS的**数据详情**提示框中展示依赖及被依赖ECS个数、首次流量次数，并可查看详细信息如下所示：

- 依赖ECS详情：单击图标，查看依赖的ECS详细信息。
- 被依赖ECS详情：单击图标，查看被依赖的ECS详细信息。
- 首次流量详情：单击图标，查看有访问关系的ECS的详细信息。

10.2.5. 日志审计

10.2.5.1. 查看事件日志

通过云防火墙的所有流量会在日志审计页面记录下来，包括流量日志和事件日志，可帮您实时审计您的网络流量并进行相应的处理。本文介绍如何查看事件日志。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**网络安全**区域单击**云防火墙**。
3. 在左侧导航栏，单击**事件日志**。
4. 在**事件日志**页签根据需要查看的防火墙类型，单击**互联网边界防火墙**、**VPC-VPC边界防火墙**或**IDC-VPC边界防火墙**。
5. 设置搜索条件，单击**搜索**。

> **说明** 如果需要查看所有事件日志，请忽略此步骤。

搜索条件	说明
源IP	设置事件的源IP地址。
目的IP	设置事件的目的IP地址。

搜索条件	说明
类型	选择事件类型。
动作	选择事件动作，支持*全部*、*观察*和*丢弃*。
时间	设置7天以内的搜索时间段。

6. 在日志列表中，查看被扫描到的时间、威胁类型、出入方向、源IP和目的IP、应用类型、严重性等级以及动作状态等信息。

10.2.5.2. 查看流量日志

通过云防火墙的所有流量会在日志审计页面记录下来，包括流量日志和事件日志，可帮您实时审计您的网络流量并进行相应的处理。本文介绍如何查看流量日志。

操作步骤

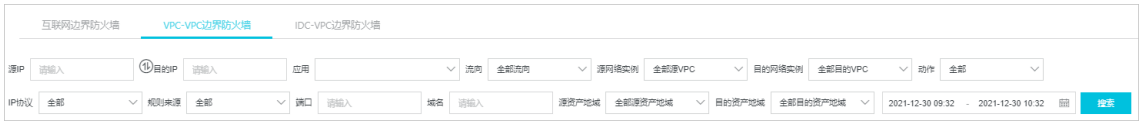
1.
2. 在顶部菜单栏，将光标放置在**安全**上，选择**网络安全 > 云防火墙**。
3. 在**云防火墙**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**云防火墙 > 流量日志**。
5. 在**流量日志**页面，单击**互联网边界防火墙**、**VPC-VPC边界防火墙**或**IDC-VPC边界防火墙**。
6. 设置搜索条件，单击**搜索**。

搜索条件	说明
源IP	设置流量的源IP地址。
目的IP	设置流量的目的IP地址。
应用	选择应用类型。
时间	设置7天以内的搜索时间段。

通过以下功能，可进一步配置搜索功能：

- **展开高级搜索**

  单击**展开高级搜索**，可以配置更多的搜索条件。



- **列表配置**

单击**列表配置**，可以设置流量列表的查看项目。



7. 在日志列表中，查看访问流量开始和结束的时间、出入方向、源IP和目的IP、应用、支持的协议、动作状态、字节数以及报文数等信息。

10.3. 数据库审计

10.3.1. 概述

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。

数据库审计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：

- **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。

- **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。

- **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。

- **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。

- **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。

- **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。

- **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。

10.3.2. 快速部署指南

10.3.2.1. 部署数据库审计系统

该章节介绍如何部署数据库审计系统。

背景信息

数据库审计系统通过镜像方式部署在服务器中。通过数据库审计系统，实现对云端自建数据库、RDS数据库访问的精确审计。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，单击**数据安全 > 数据库审计**。
3. 单击右上角**创建实例**，进入**创建实例**面板，创建数据库审计系统。



4. 设置**VPC ID**、**Vswitch ID**、**数据库实例数**等信息。
5. 联系销售人员，申请数据库审计系统正式版的License许可。

> **说明** 数据库审计系统默认提供3个月的试用License。

10.3.2.2. 配置自定义IP

本文介绍如何配置数据库审计系统的自定义IP。

背景信息

云盾用户通过自定义IP，可以在云盾安全中心直接访问数据库审计系统。

操作步骤

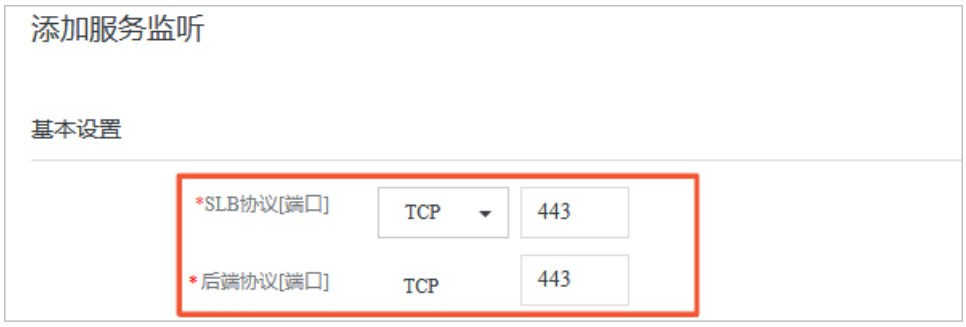
1. 登录云盾安全中心。
2. 创建数据库审计系统的SLB服务。

   具体操作，请参见*负载均衡用户指南*的**创建负载均衡实例**章节，创建负载均衡实例。

> **说明** 记录下SLB的服务地址，该地址即数据库审计系统的自定义IP。

其中，SLB的**服务监听**和**后端服务器**配置如下：

- **服务监听**：设置TCP协议和443端口，如下图所示。



- **后端服务器**：选择数据库审计系统的服务器。

3. 登录云盾安全中心。
4. 在控制台右上方，单击**安全**，选择**数据安全 > 数据库审计**。
5. 在数据库审计系统的**操作**栏，单击**管理**。
6. 在**管理**对话框中，单击**新增自定义访问地址**。
7. 输入SLB的服务地址，单击**保存**。

10.3.2.3. 登录数据库审计系统（云盾安全中心登录）

该章节介绍如何在云盾安全中心直接登录数据库审计系统。

背景信息

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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 数据库审计**
3. 在需要登录数据库审计系统的**操作**栏，单击**详情**，登录到数据库审计系统。

10.3.2.4. 数据库审计系统初始化

10.3.2.4.1. 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口。

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

10.3.2.4.2. 导入License文件

本文介绍如何导入License文件。只有导入有效License后，系统才能正常使用。

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. 选择**系统 > 证书管理**。



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。
4. 单击**上传证书**。

执行结果

校验通过后，您才可以正常使用云盾数据库审计系统。

10.3.2.4.3. 添加被审计的数据库实例

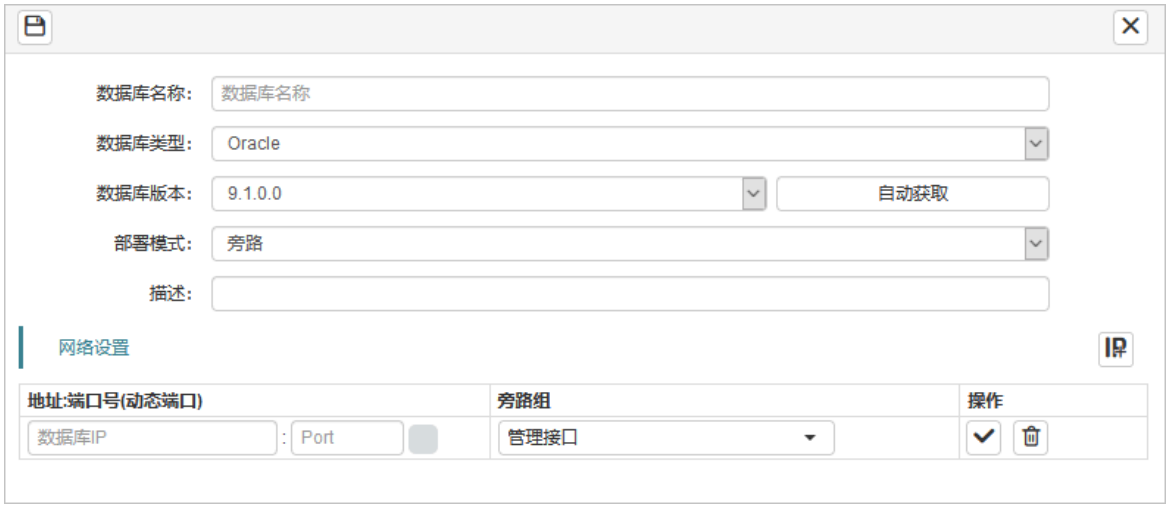
云盾数据库审计系统支持对云服务器自建数据库实例和云服务商提供的云数据库实例进行审计。

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. 在**概况**页面，单击左上角的 图标配置数据库。
3. 在**数据库列表**页面，单击**增加数据库**。

> 说明
>
> 当需要添加的数据库较多时，可在数据库列表页面，单击 图标。下载数据库模板，填写并上传。

4. 在**增加数据库**页面中，填写被审计的数据库实例的相关信息，单击左上角 图标保存。



数据库实例信息说明

参数	说明
数据库名称	为被审计的数据库实例指定一个名字。
数据库类型	选择被审计的数据库实例的类型。
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IP、端口、数据库服务名、用户名、密码，单击**确认**，系统会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）。
描述	为被审计的数据库实例添加注释。
数据库IP	○ 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。

说明 添加SQL Server数据库时，还需要输入具有一定权限的用户名及其登录密码，单击**权限校验**，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。

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。

10.3.2.4.4. 部署Agent程序

10.3.2.4.4.1. 自动部署

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。

背景信息

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。

- 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程序需要部署在使用RDS数据库的业务实例对应的应用服务器上。

操作步骤

1.
2. 在**配置**页面，单击**RMAgent组件 > RMAgent部署**，单击**安装**。
3. 在**RMAgent安装**对话框中，填写部署参数。



Agent自动部署设置

参数	说明
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`。 如果需要将Agent程序自动部署至多台服务器时，可以单击+进行添加。

> **说明**
> 添加的服务器也可以通过文件导入的方式添加，需先在文件导入页面下载模板编辑后导入。

4. 单击**确定**，即可将Agent程序自动部署到相应的服务器中。

10.3.2.4.4.2. Windows系统手动部署（应用服务与数据库服务器不同）

本章节介绍如何在应用服务和数据库部署在不同服务器的场景下手动部署Agent。

背景信息

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。

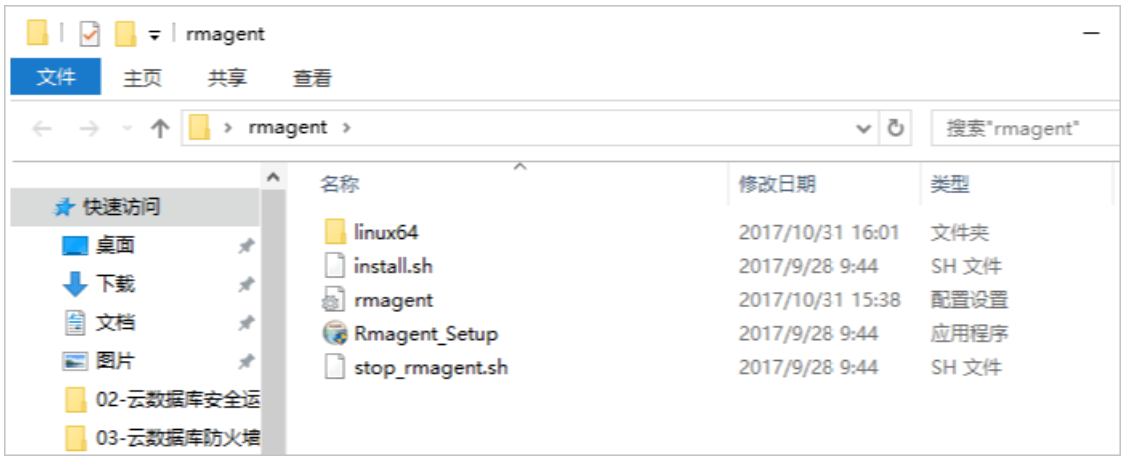
- 服务器自建数据库实例：Agent程序需要部署在数据库所在的服务器上。
- RDS数据库实例：Agent程序需要部署在使用RDS数据库的业务实例对应的应用服务器上。

操作步骤

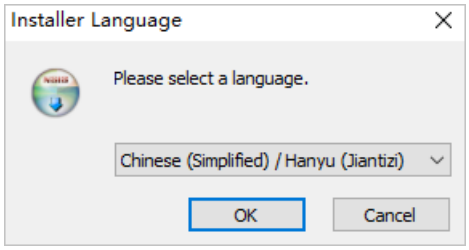
1.
2. 在**配置**页面，单击**RMAgent组件 > RMAgent部署**，单击**下载**。
   系统自动弹出Agent部署配置提示，且浏览器自动开始将Agent程序（即rmagent-dist.tar.gz文件）下载至本地。
3. 在**配置**页面，单击**RMAgent组件 > RMAgent管理**，单击右上角**白名单**。
4. 在**白名单**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**增加**。

   > **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。

5. 将Agent程序（即rmagent.tar.gz）文件上传到需要部署Agent程序的服务器，并将其解压缩。

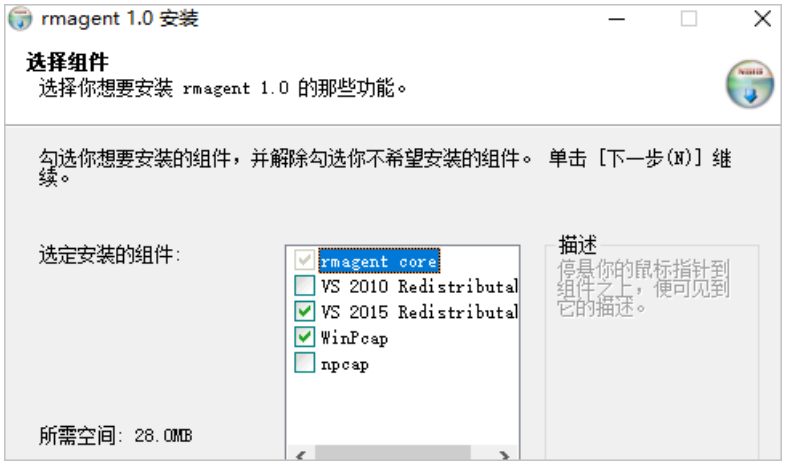


6. 打开解压后的Agent程序文件夹，双击运行Rmagent_Setup.exe程序文件。
7. 在**Installer Language**对话框中，单击**OK**。



8. 在**rmagent 1.0安装**对话框中，单击**下一步**，直到Agent程序开始安装。

   > **说明** 选择组件时，必须勾选WinPcap组件，如果选项中有VS 2015 Redistributable组件需要勾选，未勾选的组件将不进行审计。在Agent程序安装过程中会自动运行相关组件的安装程序。



9. 所有组件及Agent程序安装完成后，重新启动服务器的Windows操作系统。

10.3.2.4.4.3. Windows系统手动部署（应用服务与数据库服务器相同）

本章节介绍如何在应用服务和数据库部署在同一个服务器的场景下手动部署Agent。

背景信息

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。

- 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程序需要部署在使用RDS数据库的业务实例对应的应用服务器上。

操作步骤

1.
2. 在**配置**页面，单击**RMAgent组件 > RMAgent部署**，单击**下载**。
   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-dist.tar.gz文件）下载至本地。
3. 在**配置**页面，单击**RMAgent组件 > RMAgent管理**，单击右上角**白名单**。
4. 在**白名单**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**增加**。

   > 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。

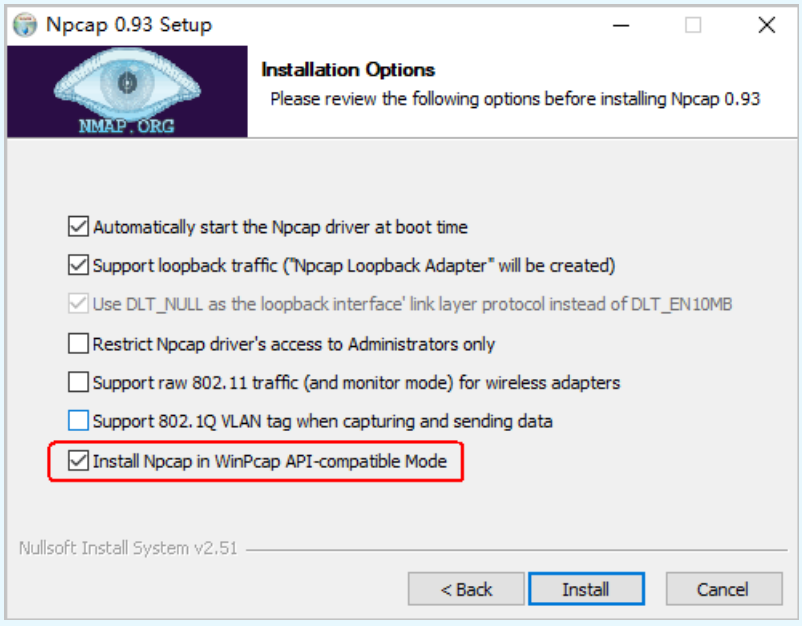
5. 将Agent程序（即rmagent.tar.gz文件）文件上传到需要部署Agent程序的服务器，并将其解压缩。
6. 打开解压后的Agent程序文件夹，双击运行Rmagent_Setup.exe程序文件。
7. 在Installer Language对话框中，单击OK。

8. 在**rmagent 1.0安装**对话框中，单击**下一步**，直到Agent程序开始安装。

> **说明**
>
> 选择组件时，必须选中npcap组件，如果选项中有VS 2015 Redistributable组件需要选中，未选中的组件将不进行审计。在Agent程序安装过程中会自动运行相关组件的安装程序。



> **说明**
>
> 安装Npcap组件时，请务必选中Install Npcap in WinPcap API-compatible Mode选项。



9. 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。



10. 重新启动服务器的Windows操作系统。

10.3.2.4.4.4. Windows系统服务器修改Agent程序连接地址

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。

操作步骤

1. 登录安装了Agent的服务器。

   根据以下两种情况登录：

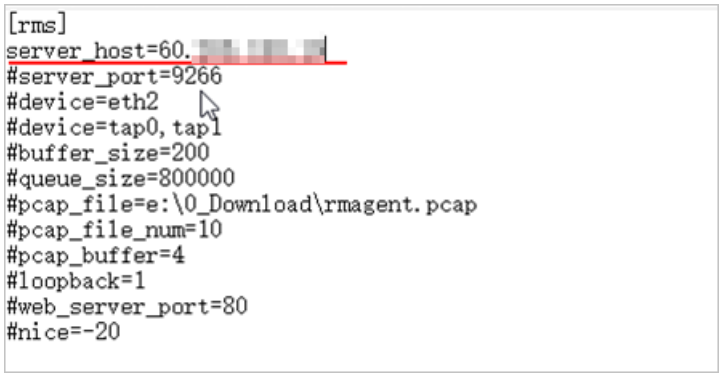
   - **服务器自建数据库实例**：登录数据库所在的服务器。
   - **RDS数据库实例**：登录RDS数据库实例所对应的应用服务器。

2. 定位到*rmagent.ini*配置文件。

   该文件路径一般为*C:\Users\用户名\AppData\Roaming\rmagent\rmagent.ini*。

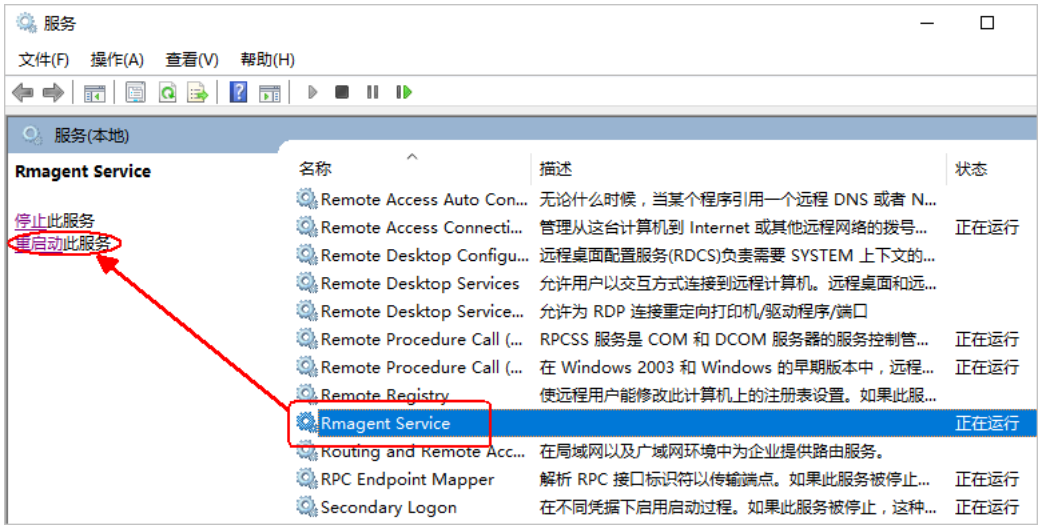
3. 编辑*rmagent.ini*配置文件，把server_host的值修改为云盾数据库审计系统的外网IP，保存文件。

   修改Agent程序连接地址

4. 重新启动rmagent服务。

   重启Agent程序服务



i. 同时按**Win+R**键，输入*services.msc*，单击**确定**。

ii. 在**服务**窗口中，选中**Rmagent Service**服务，单击**重启动此服务**。

10.3.2.4.4.5. Linux系统手动部署（应用服务与数据库服务器不同）

本章节介绍如何在应用服务和数据库部署在不同服务器的场景下手动部署Agent。

背景信息

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。

- 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程序需要部署在使用RDS数据库的业务实例对应的应用服务器上。

操作步骤

1.

2. 在**配置**页面，单击**RMAgent组件 > RMAgent部署**，单击**下载**。
   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-dist.tar.gz文件）下载至本地。
3. 在**白名单**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**增加**。

   > 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. 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，如解压rmagent.tar.gz文件所示。

解压rmagent.tar.gz文件

```
[root@rsdsdf ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  rmagent_.tar.gz
[root@rsdsdf ~]# tar -xvf rmagent_.tar.gz
./
./stop_rmagent.sh
./Rmagent_Setup.exe
./linux64/
./linux64/rmagent
./rmagent.ini
./install.sh
[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，如安装Agent程序所示。

   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），如启动Agent程序所示。

   启动Agent程序

```
[root@mysql rmagent]# cd /usr/local//rmagent/
[root@mysql rmagent]# ./rmagent
[root@mysql rmagent]#
```

10.3.2.4.4.6. Linux系统手动部署（应用服务与数据库服务器相同）

本章节介绍如何在应用服务和数据库部署在同一个服务器的场景下手动部署Agent。

背景信息

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。

- 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程序需要部署在使用RDS数据库的业务实例对应的应用服务器上。

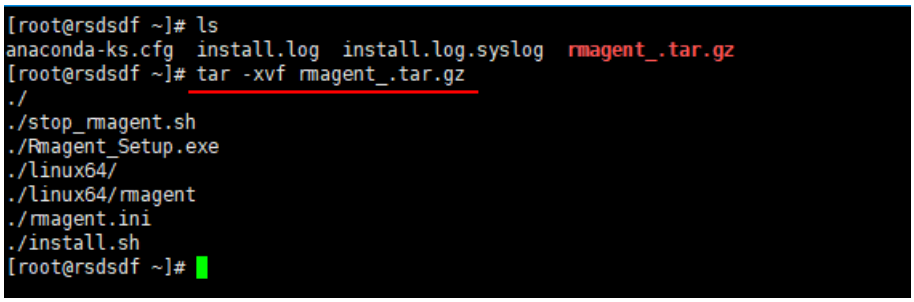
操作步骤

1.
2. 在**配置**页面，单击**RMAgent组件 > RMAgent部署**，单击**下载**。
   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-dist.tar.gz文件）下载至本地。
3. 在**配置**页面，单击**RMAgent组件 > RMAgent管理**，单击右上角**白名单**。
4. 在**白名单**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**增加**。

> 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。

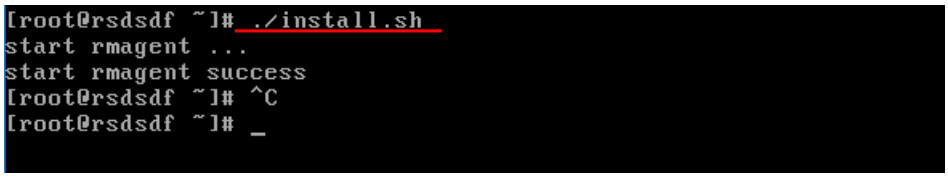
5. 以root用户登录需要安装Agent程序的服务器，将rmagent.tar.gz文件上传到服务器，并将其解压缩，如解压rmagent.tar.gz文件所示。

   解压rmagent.tar.gz文件



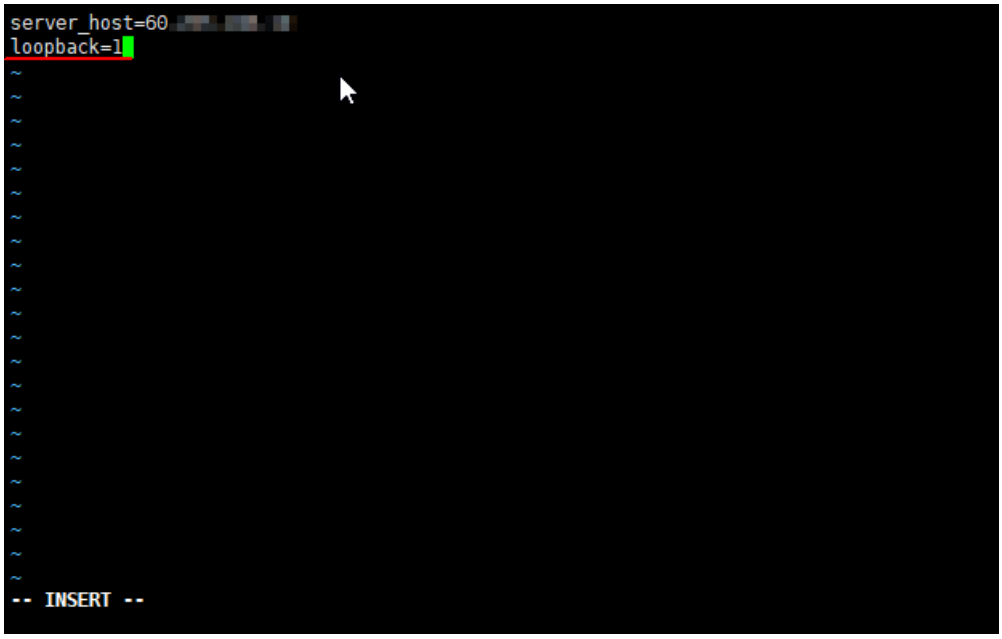
6. 执行 `chmod 755 install.sh` 命令，为install.sh文件增加权限。
7. 安装Agent程序，如安装Agent程序所示。

   安装Agent程序



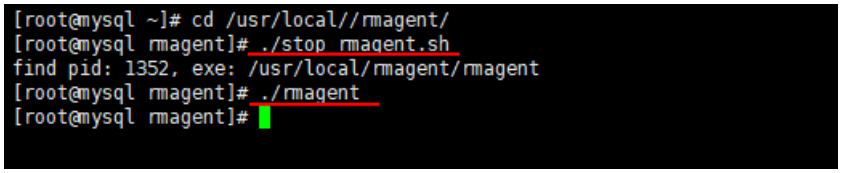
8. 安装完成后，进入rmagent安装目录，使用VI编辑器修改rmagent.ini配置文件，在文件最后加入一行 `loopback=1` ，然后保存，如修改Agent程序配置文件所示。

   修改Agent程序配置文件



9. 执行 `./stop_rmagent.sh` 命令停止rmagent进程后，执行 `./rmagent` 命令重启Agent程序，如重启Agent程序所示。

   重启Agent程序



10.3.2.4.4.7. Linux系统服务器修改Agent程序连接地址

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。

操作步骤

1. SSH方式登录安装了Agent的服务器。

   根据以下两种情况登录：

   - **服务器自建数据库实例**：登录数据库所在的服务器。
   - **RDS数据库实例**：登录RDS数据库实例所对应的应用服务器。

2. 进入*rmagent.ini*所在目录。

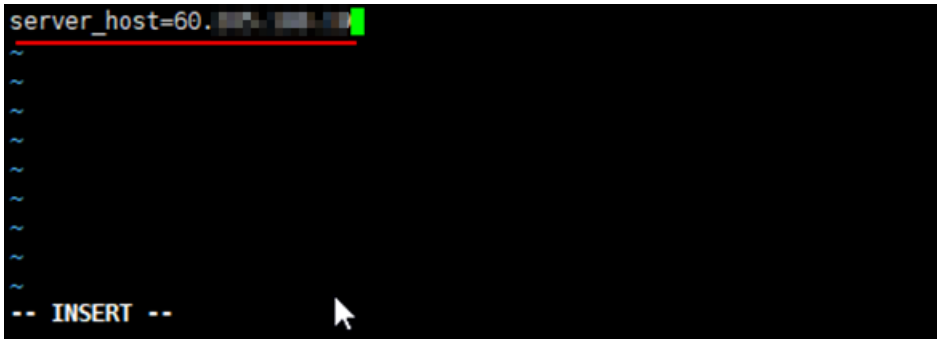
   ```
   # cd /usr/local/rmagent/
   ```

3. 编辑*rmagent.ini*配置文件。

   ```
   # vi rmagent.ini
   ```

4. 将server_host的值修改为云盾数据库审计系统的外网IP，保存文件。

   修改Agent程序连接地址



5. 重启rmagent进程。

```
# ./stop_rmagent.sh          //停止rmagent进程
# ./rmagent                  //启动rmagent进程
```

10.3.2.4.5. 部署测试

该章节介绍部署Agent后，测试数据库审计系统是否正常运行。

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。

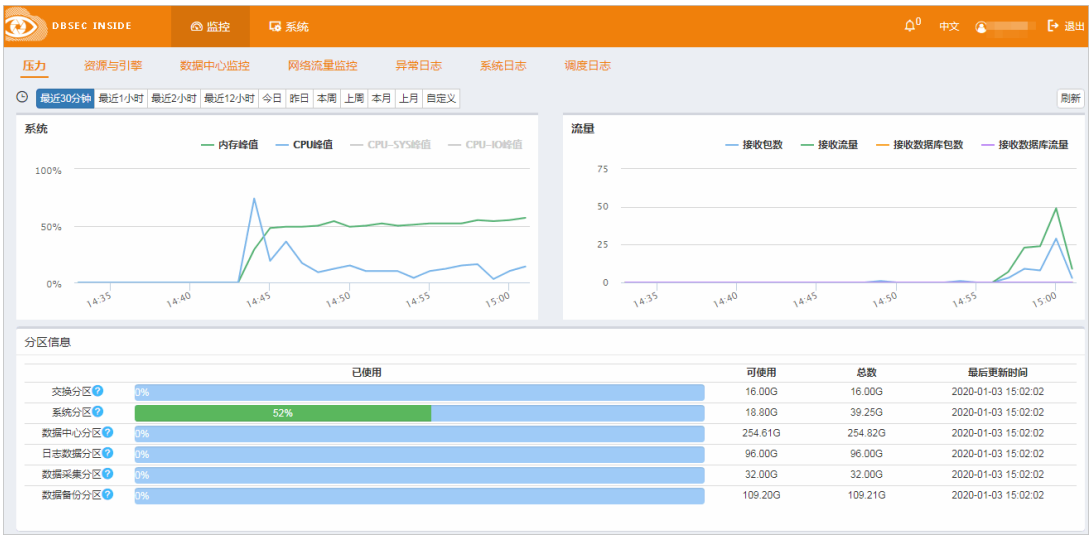
10.3.3. 系统管理员指南

10.3.3.1. 概述

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。

您需要通过系统管理员（sysadmin）账号登录云盾数据库审计系统。

系统管理页面



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

10.3.3.2. 系统管理

10.3.3.2.1. 通知管理

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。

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. 单击**系统 > 通知管理**。
3. 配置发送告警通知的Email服务器。



4. 填写完Email配置信息后，单击**保存**。
5. 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。

10.3.3.3. 监控管理

10.3.3.3.1. 压力

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。

背景信息

压力主要包括两大区域：

区域	说明
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	说明
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。

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. 单击**监控 > 压力**，选择时间周期，查看数据库审计系统的压力分析情况。

> **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。

  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。

10.3.3.3.2. 资源与引擎

在资源与引擎页面，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。
2. 单击**监控 > 资源与引擎**，查看各引擎的运行状态及资源的使用情况。

> **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。

资源与引擎



10.3.3.3.3. 数据中心监控

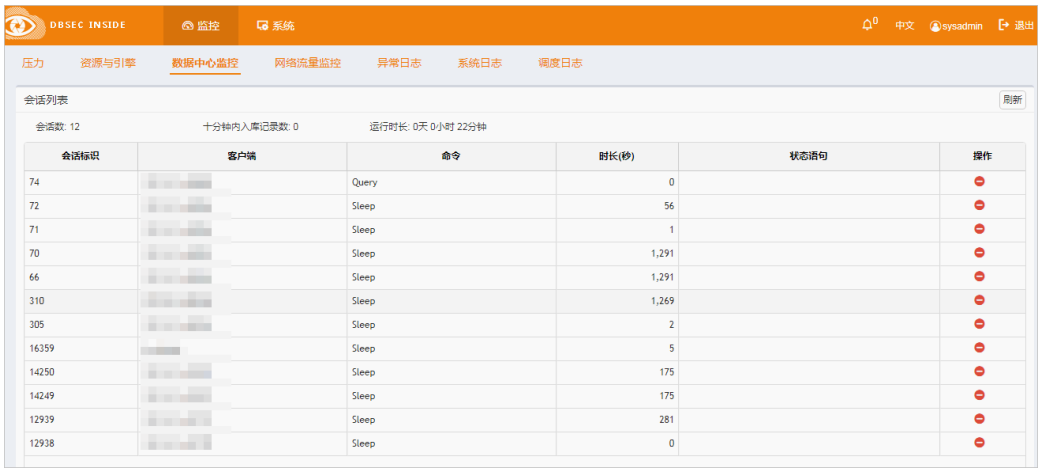
数据中心监控页面，用于监控数据中心的状态、最近十分钟入库记录数、运行时长、以及相关的会话信息等。

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. 单击**监控 > 数据中心监控**，查看数据中心监控状态。

> **说明** 单击**刷新**，可刷新数据中心实时监控状态。

数据中心监控情况



选择监控的会话，单击操作栏的⛔，可以终止该会话以释放资源。

10.3.3.3.4. 网络流量监控

网络流量监控页面，通过抓取管理接口的网络流量进行网络流量监控。

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. 单击**监控 > 网络流量监控**，查看网络流量监控状态。

> **说明** 单击**刷新**，可刷新网络流量实时监控状态。

网络流量监控



3. 选择监控文件，可进行以下操作。
   - 单击操作栏中的，删除该监控文件记录。
   - 单击操作栏中的，可将该监控文件下载到本地。

10.3.3.3.5. 异常日志

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。
2. 单击**监控 > 异常日志**。
3. 在**引擎名**下拉菜单中选择异常引擎。

> **说明** 如果选择引擎名时提示无数据，则表示没有引擎出现异常。

4. 单击**查询**，查看该引擎的异常日志记录。

   引擎异常日志



5. 选择异常日志文件，可进行以下操作。
   - 单击操作栏中的，查看异常日志文件详细信息。
   - 单击操作栏中的，删除该异常日志文件记录。
   - 单击操作栏中的，可将该异常日志文件下载到本地。

> **说明** 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。

10.3.3.3.6. 系统日志

系统日志页面记录了每个引擎运行期间的日志信息。

背景信息

系统日志页面支持查看的引擎和日志如下：

- 引擎：alw、gmon、im、npc、npp、smon、tlw、tman、dlp等。
- 日志类别：error和info。

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. 单击**监控 > 系统日志**。

   引擎系统日志



3. 在**引擎名**和**日志类型**下拉菜单中，分别选择引擎和日志类型。
4. 单击**查询**，查看该引擎的系统日志记录。
5. 选择日志文件，单击操作栏中的，可将该日志文件下载到本地。

10.3.3.3.7. 调度日志

调度日志页面记录了告警通知、报表定时推送、报表预存执行结果的日志。

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。
2. 单击**监控 > 调度日志**。



3. 设置查询日期。
4. 在**类型**和**执行结果**下拉菜单中，分别选择类型和执行结果。
5. 单击**查询**，查看该引擎的调度日志。

10.3.4. 安全管理员指南

10.3.4.1. 概述

安全管理员（secadmin）是系统的默认用户，可对安全策略进行监控、管理、制定审计。

本章节介绍通过安全管理员登录数据库审计系统的操作指导。

安全管理页面



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。

10.3.4.2. 概况

10.3.4.2.1. 系统检测

系统检测区域展示当前数据库审计系统的审计状态，包括系统语句总量、审计时长、风险分布情况等等。

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. 单击**概况**，查看当前数据库审计系统的审计状态。

   审计状态



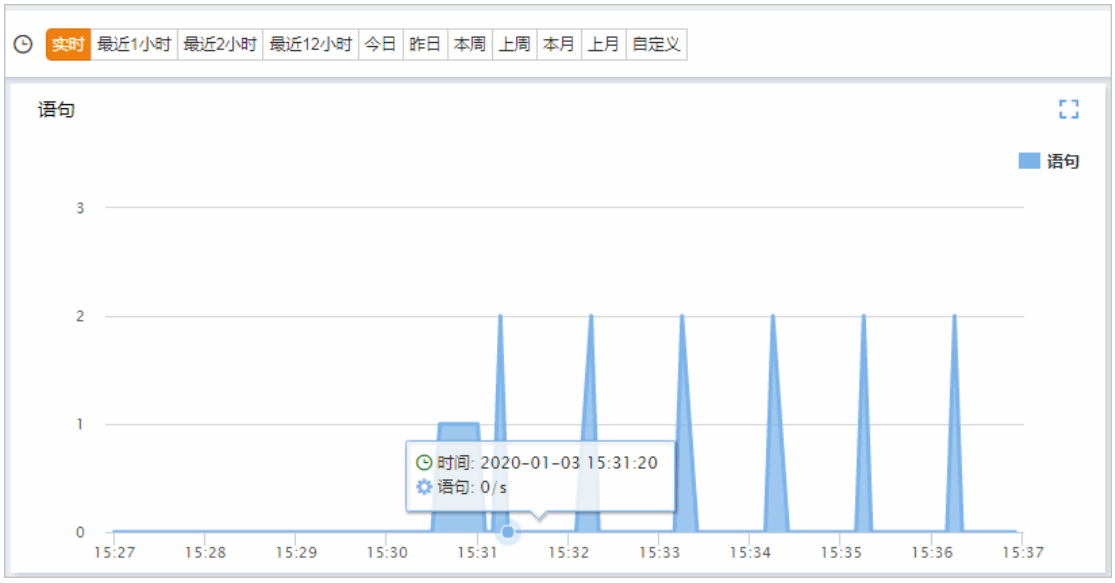
   - 实时审计状态信息如下所示，并且具有钻取功能。

状态信息	说明
运行时长	显示系统的运行时间，统计本系统自开始审计至今的总时长。
语句总量	显示并统计审计到的所有数据库语句总量。 单击**语句总量**，可查看最近执行的语句。
在线语句总量	显示系统当前的在线语句量。
今日语句量	显示并统计截止访问时间当日的审计语句量。
今日风险量	显示并统计截止访问时间当日的风险总数。
今日会话量	显示并统计截止访问时间当日的审计会话量。

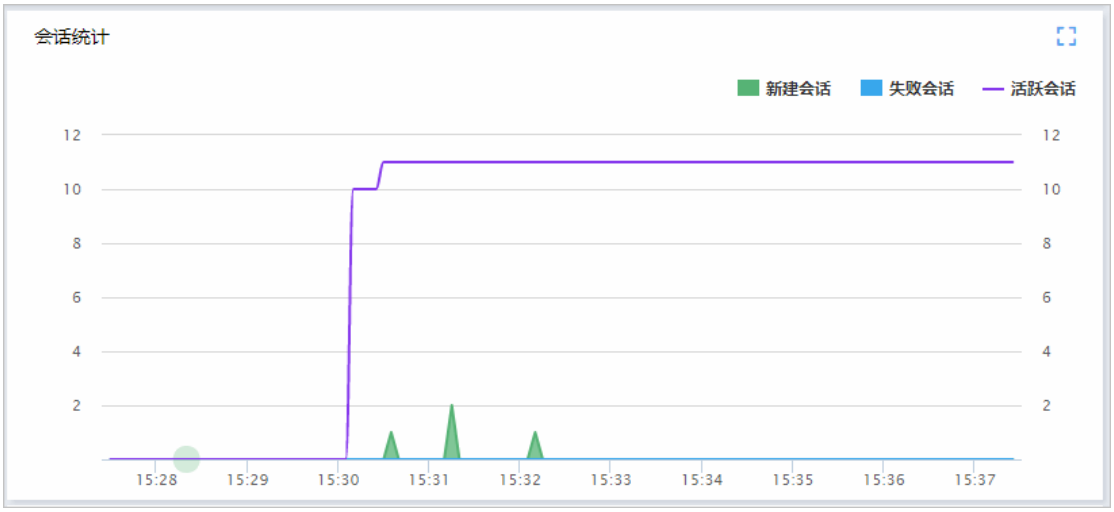
- 图形区域根据时间范围，作为统一查询维度。时间范围不同，图形的统计粒度也不同。
  - 数据库列表区域，是针对当前系统审计所有数据库的汇总展示区域，可以一览当前数据库审计全貌。数据库列表汇总展现了每条数据库的审计信息。包括：在线语句总量、在线风险量、活跃会话量、当前每秒语句量。



  - 语句分布图，以时间为单位统计某一时间范围内的语句执行情况。页面采用动态展现形式，可以通过单击统计图例的形式，根据统计需求动态展现图形。



- 会话统计基于新建会话数、失败会话数、活跃会话数等统计某一时间范围内会话数变化趋势。



10.3.4.2.2. 添加数据库

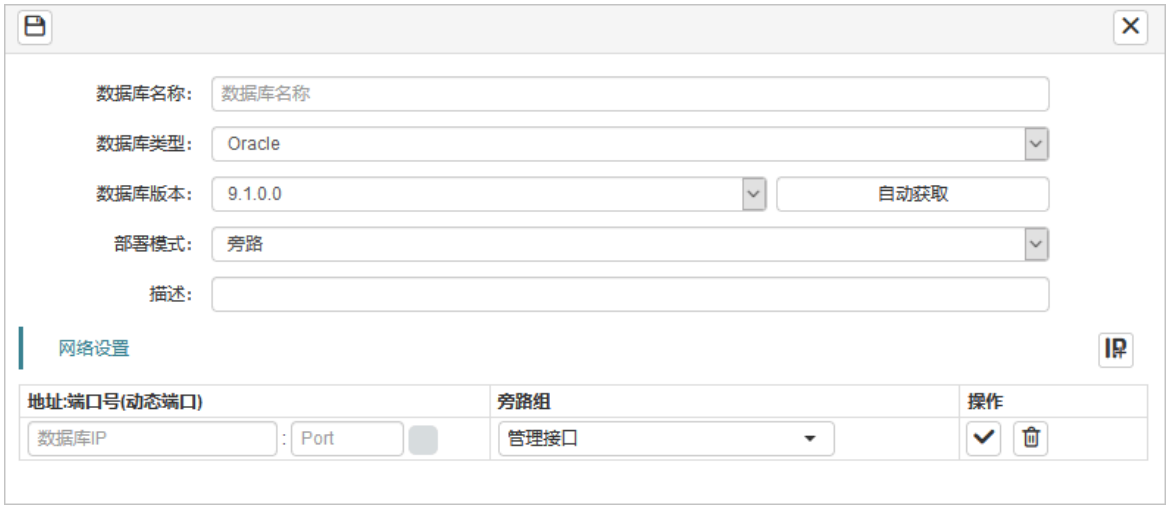
该章节介绍如何在数据库审计系统中添加待审计的数据库。

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. 在**概况**页面，单击左上角的图标配置数据库。
3. 在**数据库列表**页面，单击**增加数据库**。

> 说明
>
> 当需要添加的数据库较多时，可在数据库列表页面，单击图标。下载数据库模板，填写并上传。

4. 在**增加数据库**页面中，填写被审计的数据库实例的相关信息，单击左上角图标保存。



数据库实例信息说明

参数	说明
数据库名称	为被审计的数据库实例指定一个名字。
数据库类型	选择被审计的数据库实例的类型。
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IP、端口、数据库服务名、用户名、密码，单击**确认**，系统会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）。
描述	为被审计的数据库实例添加注释。
数据库IP	○ 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。

说明 添加SQL Server数据库时，还需要输入具有一定权限的用户名及其登录密码，单击**权限校验**，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。

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。

10.3.4.2.3. 管理已添加的数据库

背景信息

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；今日风险总量、今日语句总量；全部风险总量、全部语句总量。

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**概况**页面，单击左上角的 图标配置数据库。
3. 管理已添加的数据库。
   - 修改数据库信息：在数据库列表页面，单击。在数据库详情页面，单击。编辑后单击 保存数据库信息。
   - 删除数据库信息：在数据库列表页面，单击。

10.3.4.3. 数据库详细信息

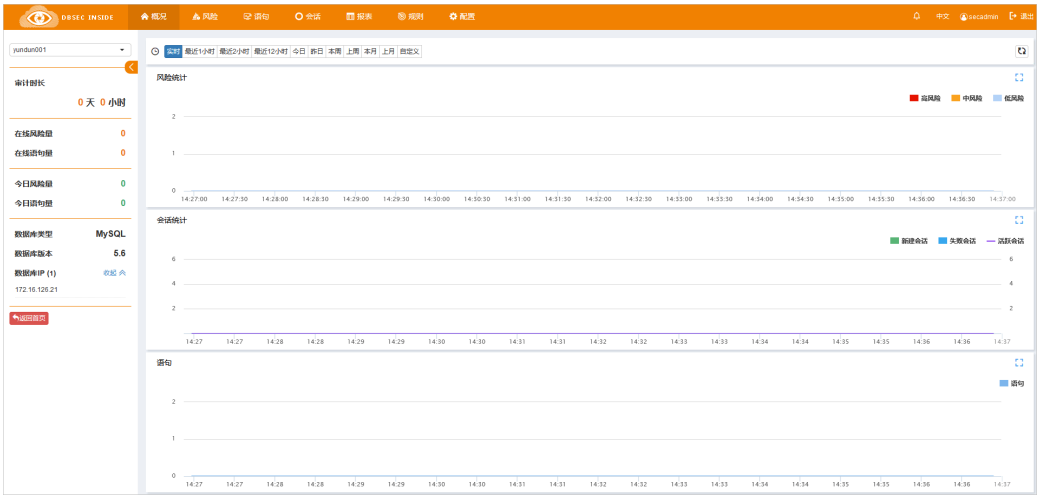
10.3.4.3.1. 概况（单库）

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，单击超链接后可跳转到对应的页面。

操作步骤

1.
2. 单击**概况**。
3. 在左侧数据库列表区域，单击已添加数据库的名称。

   单数据库概况页面



4. 在数据库详细信息页面，查看单数据库的审计状态和详情。
   - 查看单数据库的审计状态信息：

     在数据库详细信息页面，查看审计时长、语句数量等信息。

     > **说明** 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**全部数据库**，则返回数据库审计系统整体的**概况**页面。

   - 查看单数据库概况：

     选择**自定义**，设置具体时间范围，单击，可查看自定义时间范围内该数据库的风险分布、会话统计、语句情况。

10.3.4.3.2. 风险

10.3.4.3.2.1. 查看风险统计结果

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。

背景信息

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，主要包含语句规则、注入攻击、漏洞攻击、操作规则等风险。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。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，单击**风险 > 风险统计**，选择时间范围，查看风险统计图表。

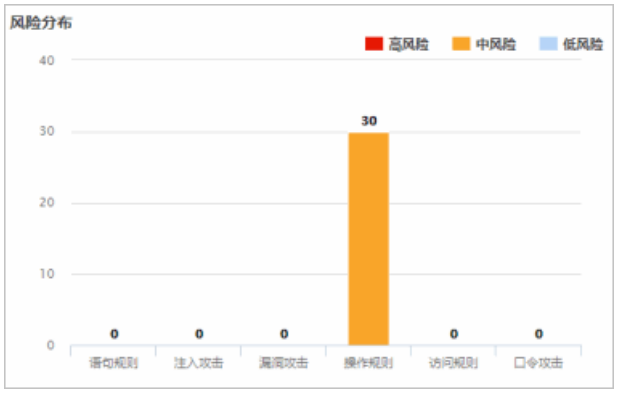
> **说明** 在**风险统计**页面的**时间**中选择自定义时间设置时间范围，单击**确定**。

- 风险统计交叉表

序号	风险类别	高风险	中风险	低风险
1	语句规则	0	0	0
2	注入攻击	0	0	0
3	漏洞攻击	0	0	0
4	操作规则	0	30	0
5	访问规则	0	0	0
6	口令攻击	0	0	0

> **说明** 单击风险统计交叉表中的蓝色数值，可跳转至**规则命中**页面查看详细分析记录。

- 风险分布图



> **说明** 风险分布图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。

10.3.4.3.2.2. 查看风险命中记录

基于对风险统计结果的延伸，风险命中页面展现每条风险记录命中规则的详细信息。

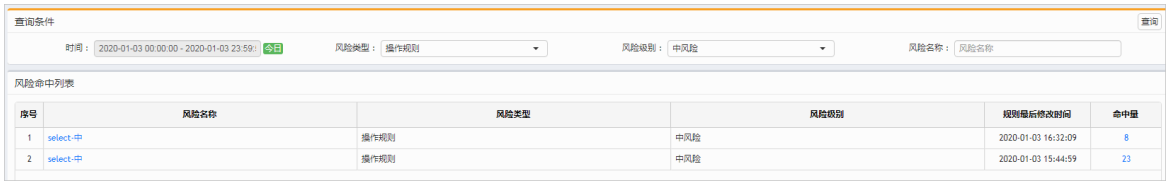
背景信息

安全管理员在**风险命中**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）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，单击数据库名称。
3. 在数据库详细信息页面，单击**风险 > 风险命中**。
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。

> **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。



5. 查看命中规则的详细信息。
   - 单击风险名称，打开**风险规则**页面，查看该规则的详细信息。
   - 查看风险命中详情。
     a. 单击命中数量，打开**命中列表清单**页面。

        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。
     b. 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。
     c. 设置搜索条件，单击**查询**，可查询特定的风险语句记录。
     d. 单击**导出**，设置导出行数，导出风险命中列表详情信息。

        > **说明** 导出的文件格式为.csv，文件名默认为数据信息。

10.3.4.3.2.3. 检索风险语句

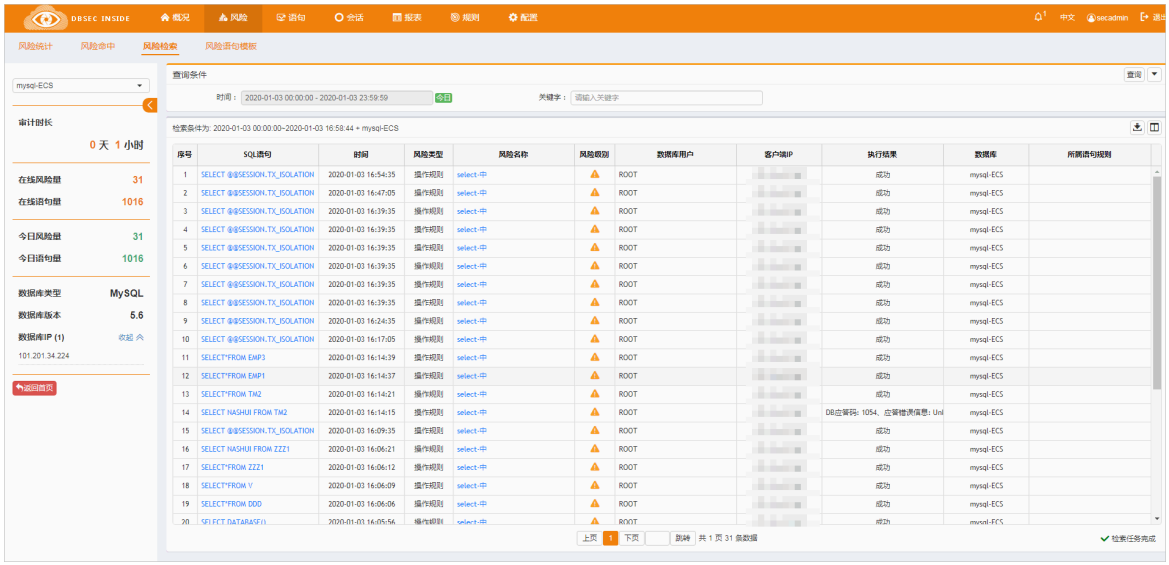
风险检索是风险设置的核心组件，以列表清单的方式逐条展现风险语句的详情。

背景信息

风险语句的详细信息包括具体的SQL语句、（触发）时间、风险类型、风险名称、风险级别、数据库用户、客户端IP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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，单击**风险 > 风险检索**，选择查询时间范围，查看风险语句记录。



10.3.4.3.2.4. 查看风险语句模板

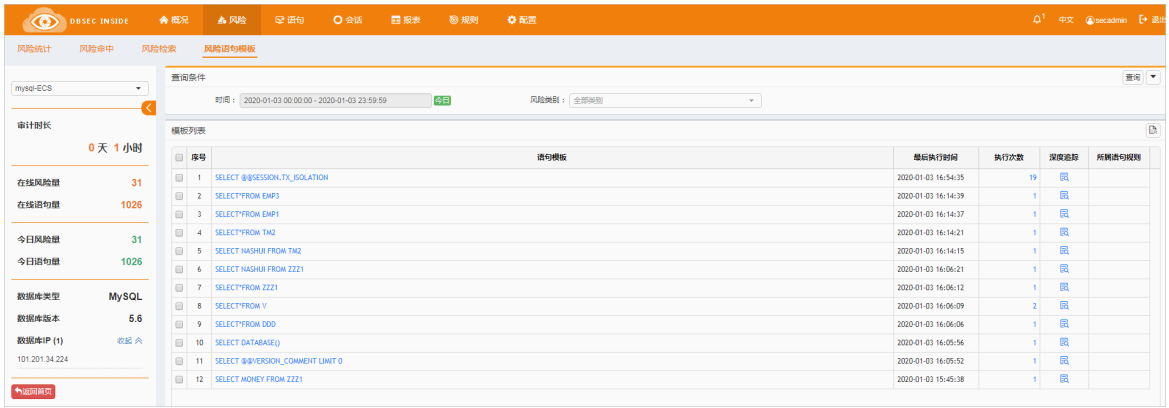
风险语句模板是命中风险的语句模板，去掉prepare参数、查询参数、注释、多余空格、换行之类的参数，其他格式一样的语句，归类为一种语句模板。

背景信息

使用风险语句模板可以大大的减少存储空间，提高查询速度。通过语句模板可直接添加语句规则。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，单击**风险 > 风险语句模板**，选择查询时间范围、风险类别，查看风险语句模板。



4. 单击语句模板所在行的  ，可以查看访问来源及语句详情。
5. 单击  可将语句模板添加至语句规则。

   语句模板处理可选择**已勾选**或**按查询结果**。

   - 已勾选：将模板列表中选中的语句模板添加至语句规则。

- 按查询结果：将模板列表中查询到的所有语句模板添加至语句规则。



10.3.4.3.3. 语句

10.3.4.3.3.1. 查看SQL统计

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。

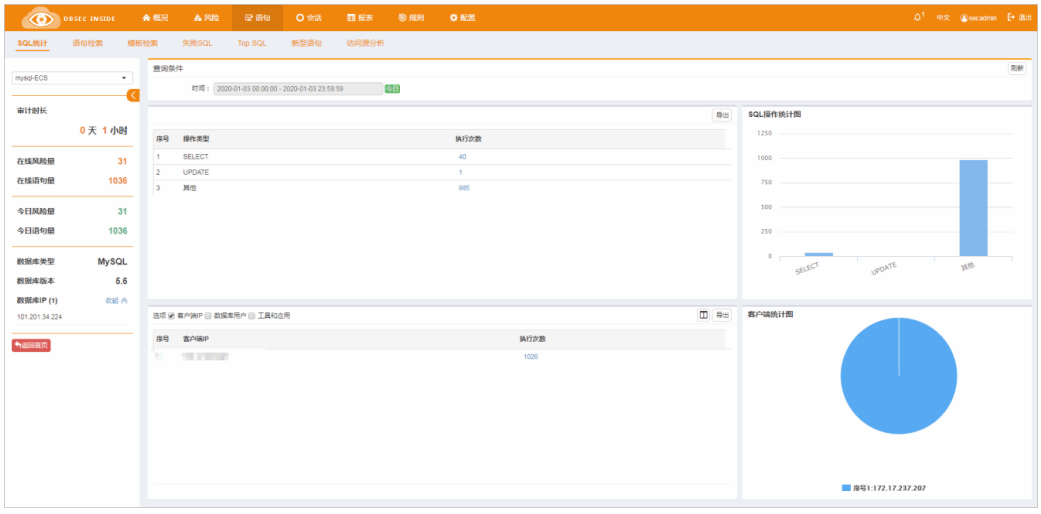
背景信息

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。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 单击**语句 > SQL统计**，选择查询时间范围，查看操作类型及语句来源统计结果。

   SQL统计页面



10.3.4.3.3.2. 检索SQL语句

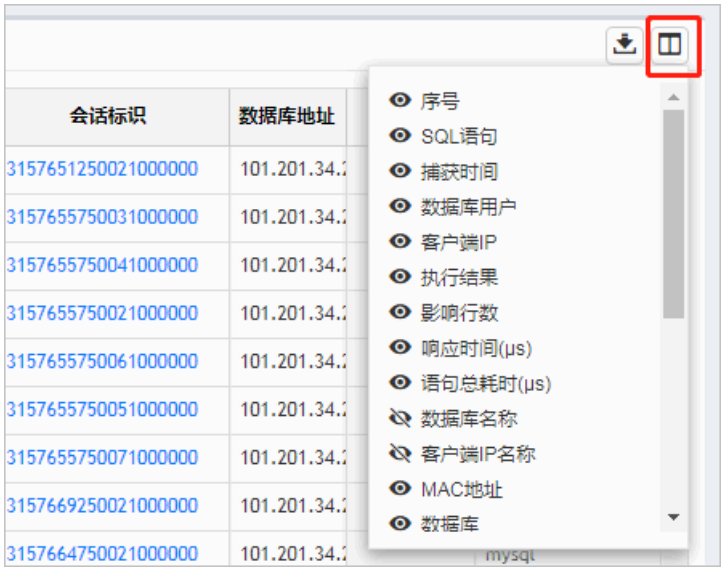
在**语句检索**页面，安全管理员可以以时间为语句检索条件检索本系统审计的SQL语句。

操作步骤

1.
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，单击数据库名称。
3. 单击**语句 > 语句检索**，选择查询时间范围。
4. 单击，设置检索条件，单击**查询**。

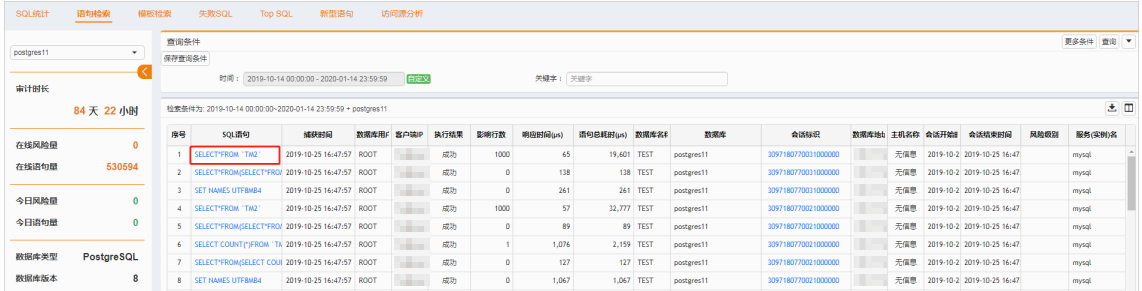
> 说明 单击**更多条件**，在**检索条件设置**对话框中，可添加更多检索条件。

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。



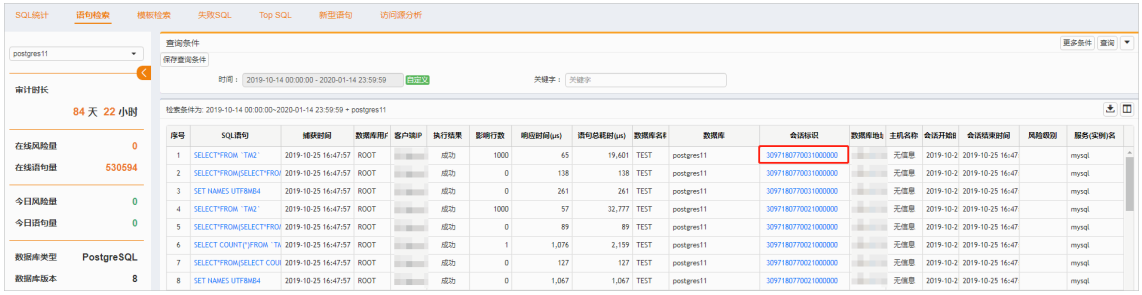
   - 单击右上角，选择**csv下载**，可将当前语句列表导出到本地。

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。
   - 通过单击SQL语句链接，进入语句详情页面。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。



   - 通过单击会话标识链接，进入会话详情列表。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。



> **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。

7. 在语句详情页面，单击**语句模板**区域的，可将SQL语句纳入现有的语句规则中。

10.3.4.3.3.3. 检索语句模板

在**模板检索**页面可以对SQL语句模板进行查询。

背景信息

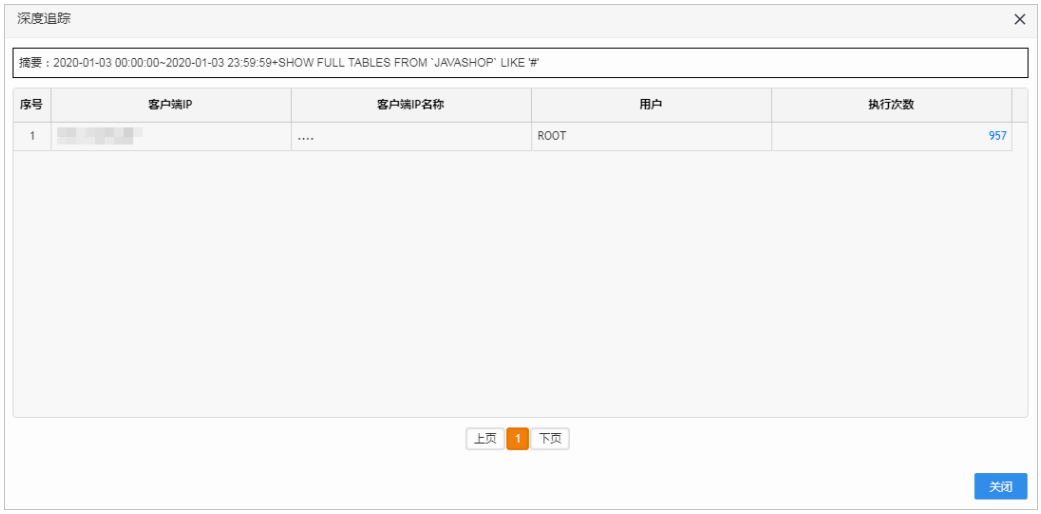
本系统采用语句模板的方式将SQL语句进行归纳整理，通过简化的SQL语句结构，对同一类SQL语句进行记录。安全管理员通过模板检索功能，可以快速定位高危SQL语句信息。

操作步骤

1. 使用安全管理员（secadmin）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，单击数据库名称。
3. 单击**语句 > 模板检索**，选择查询时间范围，单击**查询**。

   查看语句模板列表，包括语句模板、最后执行时间、执行次数等信息。
4. 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。

   深度追踪信息



5. 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。

10.3.4.3.3.4. 查看执行失败的SQL语句

在查看执行失败SQL语句的页面可以查看选定时间内所有执行失败的语句。

背景信息

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）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，单击数据库名称。
3. 单击**语句 > 失败SQL**，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 ，可以选择列表项展示内容。

     失败SQL列表展示列设置

   - 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。
   - 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。

     查看语句详情



- 单击列表右上角的，选择csv下载，可将当前列表中的失败SQL语句信息导出。

10.3.4.3.3.5. 查看TopSQL语句

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

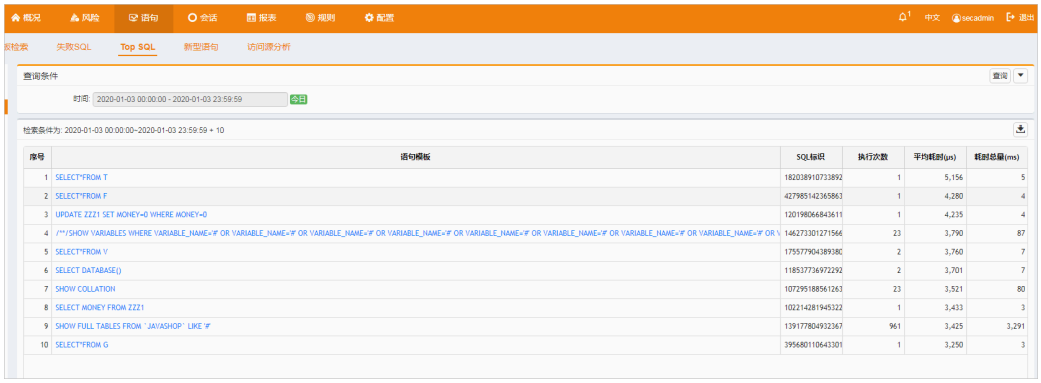
1. 使用安全管理员（secadmin）登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 单击**语句 > Top SQL**，选择查询时间范围，单击**查询**。

   TopSQL页面支持以下查询条件。

查询条件	说明
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。

   查看Top SQL语句统计情况



- 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，选择csv导出，可将当前列表中的Top SQL语句导出。

10.3.4.3.3.6. 查看新型语句

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。

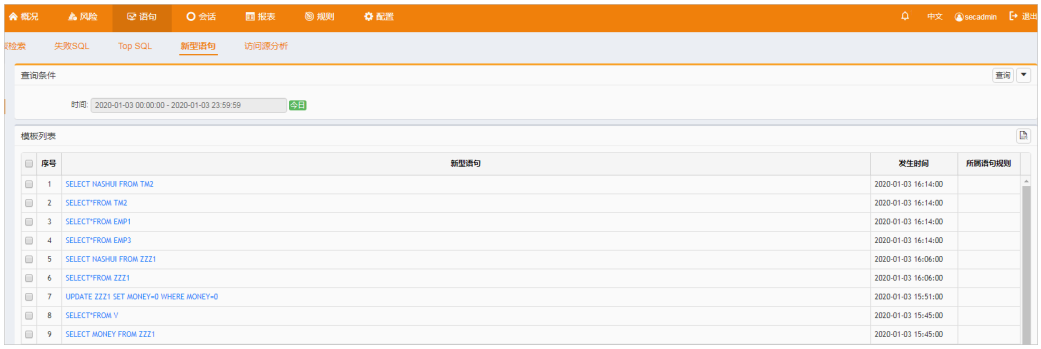
背景信息

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）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，单击数据库名称。
3. 在数据库详细信息页面，单击**语句 > 新型语句**，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。

   查看新型语句



> **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。

10.3.4.3.3.7. 分析访问源

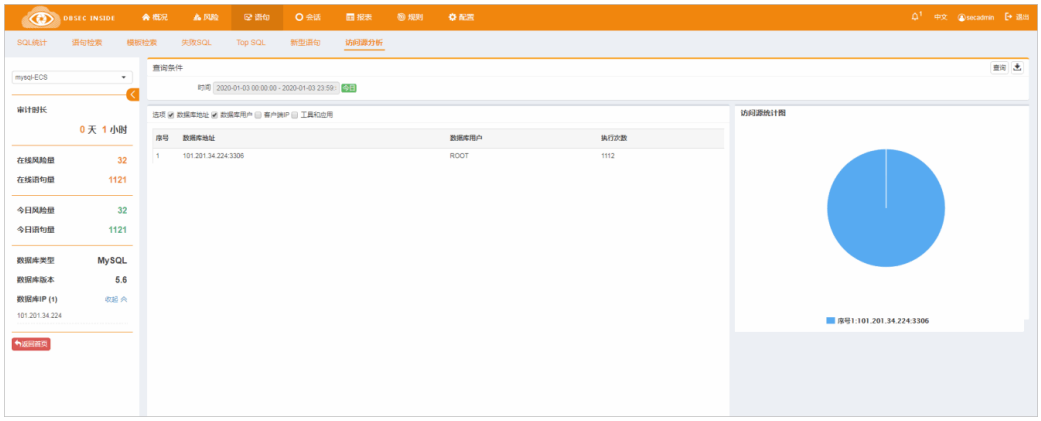
访问源分析页面主要用于统计所访问数据库地址、数据库用户、客户端地址、工具和应用等信息。

操作步骤

1. 使用安全管理员（secadmin）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，单击数据库名称。
3. 单击**语句 > 访问源分析**，选择查询时间范围，查看访问源分析结果。

> **说明** 选中数据库地址、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，支持多维度分析。

查看访问源分析结果



- 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。

10.3.4.3.4. 会话

10.3.4.3.4.1. 查看会话统计

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。

背景信息

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。

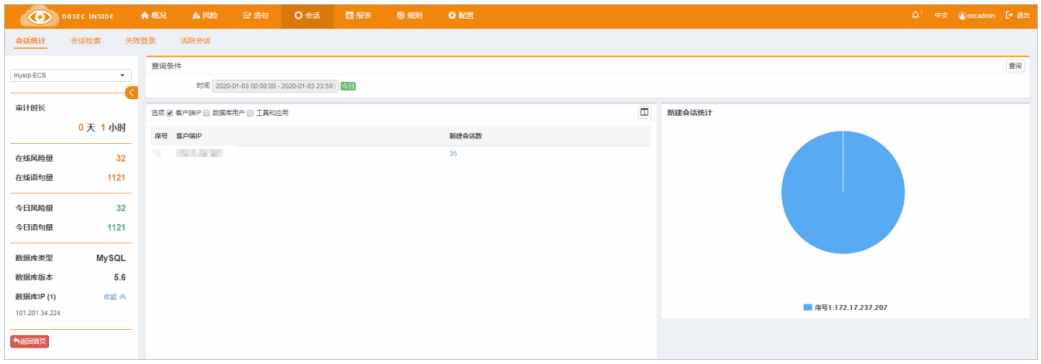
操作步骤

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。

3. 单击**会话 > 会话统计**，选择查询时间范围，单击**查询**，查看会话统计情况。

> **说明** 选中客户端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。

查看会话统计结果



- 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。

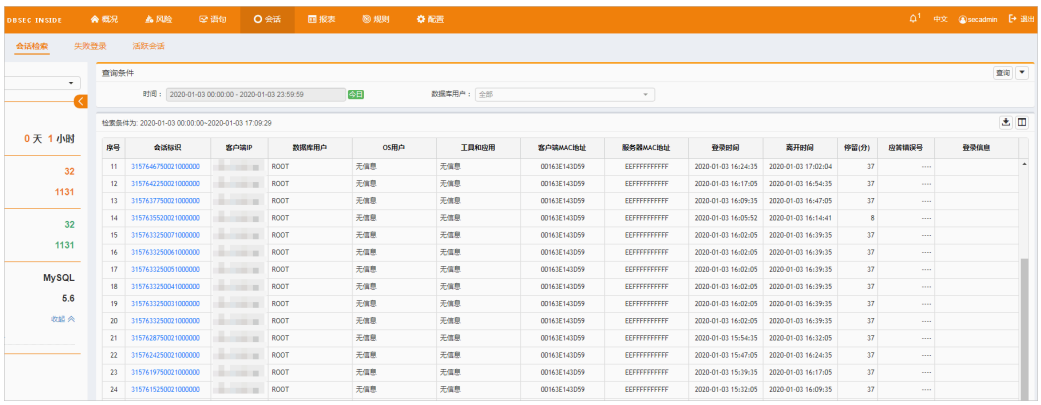
10.3.4.3.4.2. 检索会话信息

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。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 单击**会话 > 会话检索**，选择查询时间范围，单击**查询**，检索会话信息。

会话检索页面



> **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。

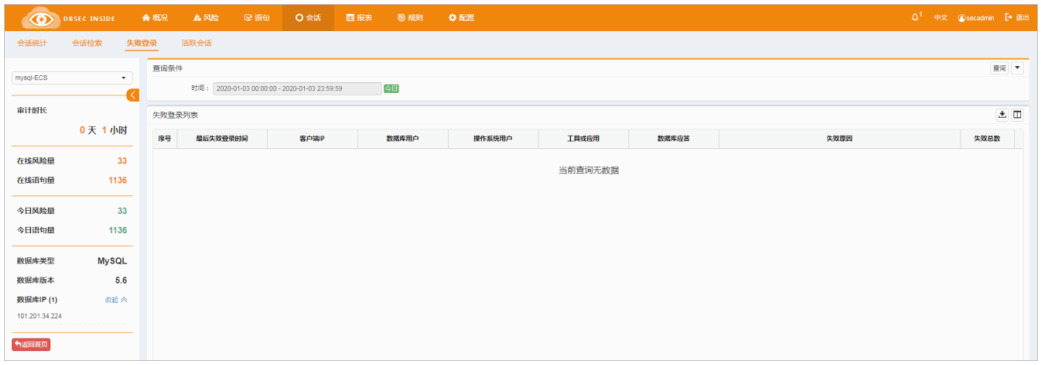
10.3.4.3.4.3. 查看登录失败会话

在失败登录页面可以通过网格式报表查看登录失败的会话信息及统计的失败总数。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 单击**会话 > 失败登录**，选择查询时间范围，单击**查询**，查看登录失败的会话信息。

   失败登录页面



- 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。
- 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。

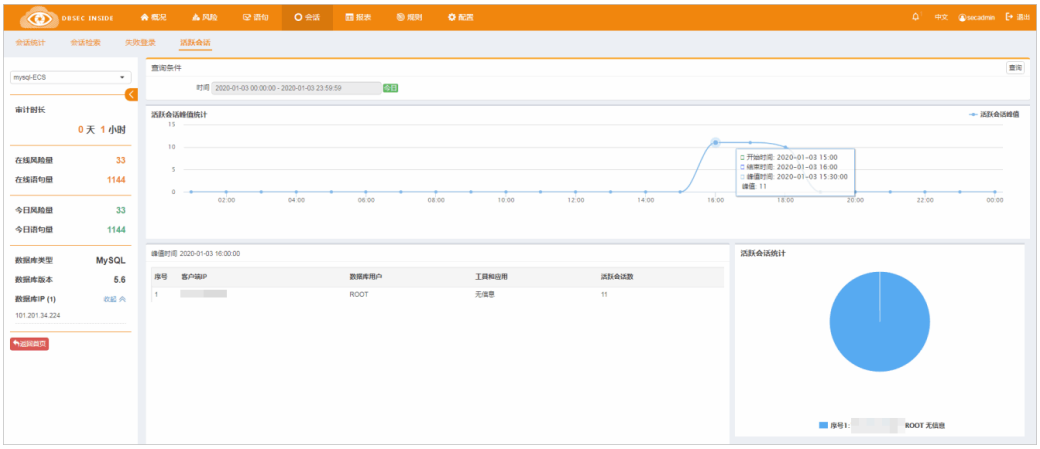
10.3.4.3.4.4. 查看活跃会话

活跃会话页面通过活跃会话趋势图、活跃会话统计表、活跃会话统计图对某一时间段内较为活跃会话进行统计、展示。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 单击**会话 > 活跃会话**，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。

   活跃会话页面



10.3.4.3.5. 报表（单库）

10.3.4.3.5.1. 查看报表（单库）

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。

背景信息

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。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 定位到**报表**，根据需要选择报表类型页签，选择模板类型、时间范围，单击**预览**，查看该数据库对应的报表。
   - 综合报表
     - 报表名称：综合状态报告
     - 报表类型：日报、周报、月报
     - 报表内容：风险分布状况、客户端统计分析、语句统计分析、性能状况等
     - 统计图展现形式：柱形图、曲线图、双轴折线图等



- 合规报表
  - 报表名称：SOX-萨班斯报告
  - 报表类型：SOX-萨班斯报告、PCI报告、等保参数报告
  - 报表内容：风险分布状况、语句统计分析等
  - 统计图展现形式：柱形图等



- 专项报表
  - 报表名称：风险综合分析报告
  - 报表类型：风险分布统计报告、客户端风险分析报告、语句访问类型分布报告、数据库概要分析报告等
  - 报表内容：风险分布状况等
  - 统计图展现形式：柱形图等



4. 设置报表定时推送。
   i. 单击**加入定时推送任务**。
   ii. 选择**推送任务**、**推送语言**，填写**报表名称**，选择**报表格式**。
   iii. 单击**添加**。
5. 单击**导出**，根据需要选择文档格式。
   导出格式支持Word、PDF、HTML。
6. 单击**导出**

10.3.4.3.5.2. 设置报表预存

通过报表预存功能可以对各类报表按照每年、每周或每月的周期进行预存。

背景信息

已预存的报表可留存3个月时间。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，单击**报表 > 报表预存**。
4. 单击**预存设置**。
5. 在**预存设置**页面，在需要设置预存周期的报表模板后单击**设置**。



6. 选择需要设置的时间单位，单击**保存**。

   时间单位可选择**每年**、**每月**或**每周**。

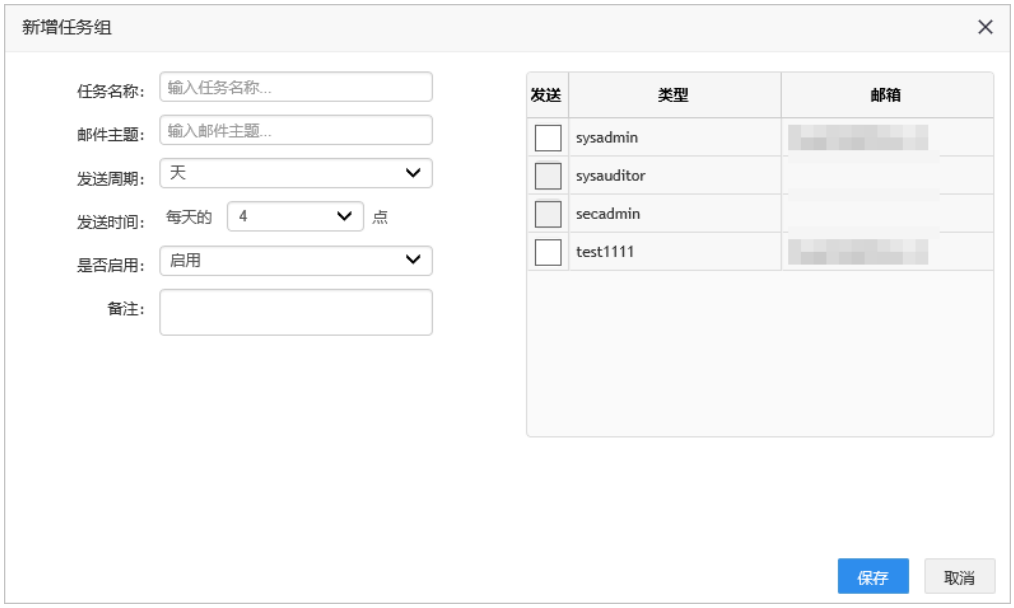
10.3.4.3.5.3. 管理定时推送任务（单库）

该章节介绍如何管理单数据库的推送任务组和推送任务。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，定位到**报表**页面。
4. 单击**定时推送**，管理定时推送任务。
   - 新增定时推送任务组

     单击**添加**，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**。



- 修改任务组

  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。

- 删除任务组

  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。

- 查看、修改和删除报表推送任务

  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。

- 查看报表历史记录

  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。

10.3.4.3.6. 规则（单库）

10.3.4.3.6.1. 设置漏洞攻击规则

针对利用“数据库漏洞”进行数据库攻击的行为告警，虚拟补丁列表显示所有支持的数据库版本下的所有漏洞攻击规则。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，单击**规则 > 漏洞攻击**，设置漏洞库类型、风险级别等查询条件，单击**查询**，查看对应的虚拟机补丁列表。
4. 单击漏洞补丁所在行**状态**列的设置按钮，可以启用或禁用漏洞补丁。

> **说明** 也可选中多个漏洞补丁后，单击右上角的**批量启用**、**批量禁用**，进行统一设置。

10.3.4.3.6.2. 设置语句规则

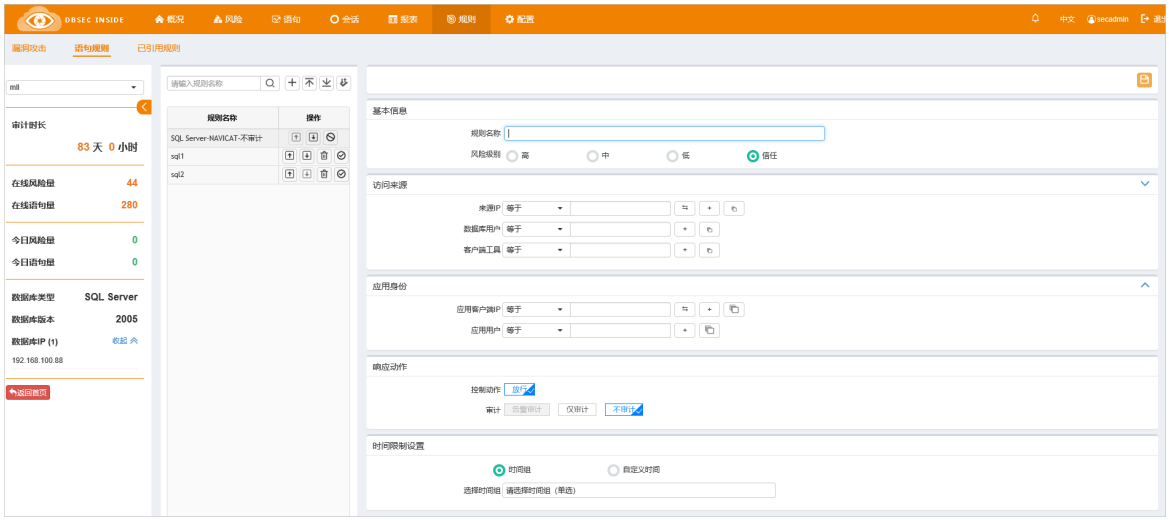
对指定数据库审计语句统一添加信任、风险规则。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面，单击**规则 > 语句规则**。
4. 单击＋，设置规则参数。

   规则参数说明

参数	说明
规则名称	必填项，填入规则名称。
风险级别	必选项，等级包括高、中、低、信任，系统默认为中级。该规则触发时，会产生一条对应等级的风险告警。
来源IP	可填项，指访问业务类型的客户端IP地址。若从内网访问，则对应其内网IP地址，若从公网访问，则对应其公网IP地址。 可设置单个IP，也可设置IP段，可添加多个。
数据库用户	可填项，数据库用户名，可设置多个，支持等于、不等于、包含、不包含、正则等方式。
客户端工具	可填项，定义规则作用的客户端工具，可设置多个，支持等于、不等于、包含、不包含、正则等方式。
应用客户端IP	可填项，需部署应用关联才可使用。
应用用户	可填项，需部署应用关联才可使用。
时间限制设置	可从事先定义的时间组中选择，也可自定义时间段。



5. 单击右上角的  ，保存新增的语句规则。

   规则保存成功后，根据界面提示选择是否需要关联语句模板。

10.3.4.4. 报表

10.3.4.4.1. 查看报表

本章节主要介绍数据库审计系统的全局报表。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。

背景信息

关于数据库单库报表说明，请参见查看报表（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。

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，在数据库列表区域，选择已添加的数据库，单击数据库名称。
3. 在数据库详细信息页面定位到**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。
   - 综合报表
     - 报表名称：综合状态报告
     - 报表类型：日报、周报、月报
     - 报表内容：风险分布状况、客户端统计分析、语句统计分析、性能状况等
     - 统计图展现形式：柱形图、曲线图、双轴折线图等
   - 合规报表
     - 报表名称：SOX-萨班斯报告
     - 报表类型：SOX-萨班斯报告、PCI报告、等保参数报告

- 报表内容：风险分布状况、语句统计分析等
- 统计图展现形式：柱形图等

- 专项报表
  - 报表名称：风险综合分析报告
  - 报表类型：风险分布统计报告、客户端风险分析报告、语句访问类型分布报告、数据库概要分析报告等
  - 报表内容：风险分布状况等
  - 统计图展现形式：柱形图等



4. 设置报表定时推送。
   i. 单击**加入定时推送任务**。
   ii. 选择推送任务，填写报表名称，选择报表格式。
   iii. 单击**确定**。
5. 导出报表。
   i. 单击**导出**。
   ii. 选择导出格式。

   > **说明** 报表支持以Word、PDF、HTML格式导出。

   iii. 单击**确定**。

10.3.4.4.2. 管理定时推送任务

该章节介绍如何管理推送任务组和推送任务。

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**报表**页面，单击**定时推送**，管理定时推送任务。
   - 新增定时推送任务组

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，选中需要发送的用户，单击**保存**。

- 修改任务组

  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。

- 删除任务组

  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。

- 查看、修改和删除报表推送任务

  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。

- 查看报表历史记录

  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。

10.3.4.5. 系统告警信息

10.3.4.5.1. 查看系统告警信息

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。

操作步骤

1. 单击页面右上角的。



2. 在**系统告警信息**对话框，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。

   > **说明** 在描述栏中可查看该告警信息的具体触发原因。

3. 检查并处理该系统异常后，单击操作栏中的，该信息将不再告警。

10.3.4.5.2. 配置系统告警

系统告警信息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。

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. 单击**配置 > 告警设置 > 邮件通知**。



3. 单击右上角的＋，在**模板信息**中设置**邮件标题**、**模板名称**等告警邮件信息。
4. 单击**模板内容**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. 单击**保存**，完成系统告警邮件配置。

10.3.4.6. 配置

10.3.4.6.1. 用户管理

该章节介绍如何管理数据库审计系统的用户。

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**配置**页面，单击**用户管理**，管理数据库审计系统用户。

> **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。

- 添加用户

  单击右上角的＋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，即添加新用户。

- 修改用户信息

  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。

- 删除用户

  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。

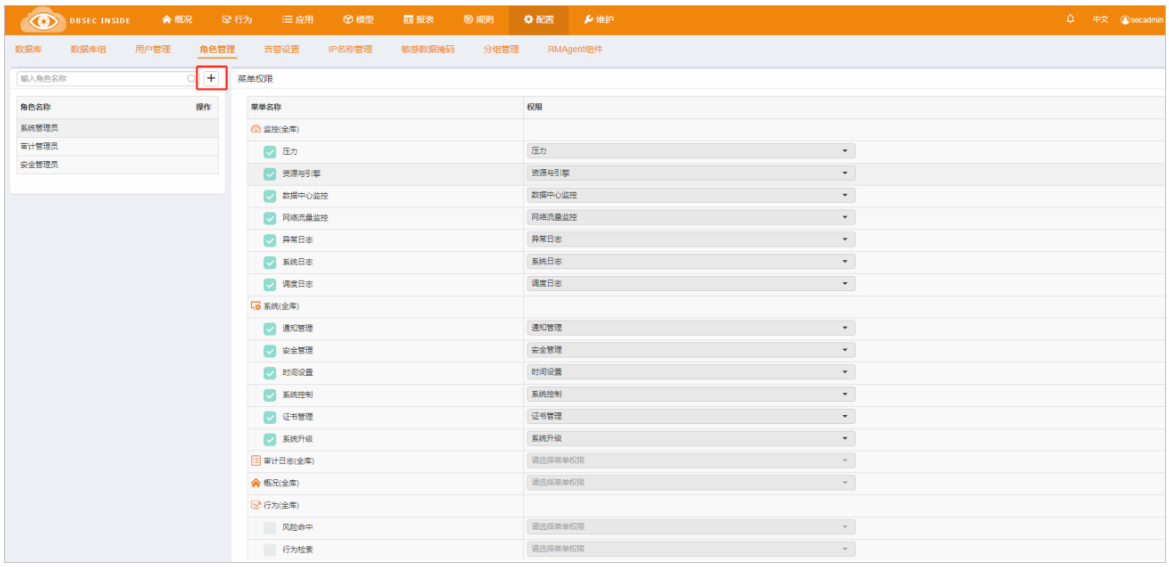
10.3.4.6.2. 角色管理

该章节介绍如何为角色进行功能授权。

操作步骤

1. 单击**配置 > 角色管理**。
2. 在左侧角色列表选择需要设置权限的角色，在右侧**菜单权限**区域设置该角色的权限。

   可以单击界面左侧 ＋，添加新角色。



> **说明** 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。

3. 单击**保存**，单击**确定**。

10.3.4.6.3. IP名称管理

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）登录云盾数据库审计系统。
2. 单击**配置 > IP名称管理**。
3. 管理IP名称。
   - 添加IP名称

     单击右侧 ＋ 增加按钮，在**编辑业务化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。
   - 导入IP名称

     单击右侧 导入按钮，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。

> **说明** 在**导入IP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。

- 导出IP名称

  单击 导出按钮，可将当前IP业务化列表以CSV格式导出至本地。

- 查询IP名称

  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。

10.3.4.7. 维护

10.3.4.7.1. 数据备份恢复

10.3.4.7.1.1. 设置自动备份

数据库审计支持对审计日志进行自动备份，确保审计日志的安全性和永久性。

背景信息

审计日志支持对备份存储进行定制，可减少系统存储的压力。同时，支持日志恢复功能，方便您随时对备份数据进行查询和恢复。

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. 单击**维护 > 数据备份恢复**。
3. 在**自动备份配置**区域，设置开始备份时间、备份策略，选择是否上传服务器，服务器类型。



   - **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。
   - **备份策略**：自动备份默认备份3天前的数据，即备份自当天起3天前的数据。例如，在12月17日，自动备份默认备份12月15日当天的审计日志数据。
   - **上传服务器**：备份的审计日志，出于安全性和数据盘空间考虑支持选择自动上传到指定服务器。目前支持FTP、SFTP和NFS服务器。

     说明 设置FTP服务器时，FTP路径是FTP服务器下的已有目录，而不是FTP服务器在操作系统上的存储目录。

4. 单击**保存**。

10.3.4.7.1.2. 手动备份与恢复

该章节介绍如何手动备份和恢复当前系统配置数据。

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. 单击**维护 > 数据备份恢复**。
3. 在**系统配置信息备份/恢复**，单击**备份**。



4. 单击**确定**，对当前系统配置数据进行备份。

后续步骤

备份成功后，在**系统配置信息备份/恢复**区域，单击**恢复**并选择备份文件后，单击**确认**。

> 警告 该备份的系统配置数据会覆盖当前系统配置数据。

10.3.4.7.1.3. 查询备份清单

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操作记录。

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. 单击**维护 > 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**服务器类型**。

   可选服务器类型包含**FTP**、**SFTP**和**NFS**。
5. 选择数据状态。

   可选择的数据状态如下。
   - **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。
6. 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。

10.3.4.7.2. 自动清理告警与数据

设置在线数据的清理门限（即阈值）与备份数据的告警门限和清理门限、自动清理间隔以及开始时间，当审计日志和备份文件达到上限后系统将自动启动清理。

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. 单击**维护 > 告警与数据清理**。
3. 根据需要，设置清理门限及清理周期。



   - **清理门限**：达到指定条数后，将清理旧的数据。
   - **告警门限**：当前产品数据盘分配的数据分区空间不足某值，如40%时生成系统告警。
   - **清理门限**：当前产品数据盘分配的数据分区空间不足某值，如50%时清理备份数据，释放存储空间。
   - **自动检查周期**、**清理开始时间**：默认每一周期内（天、时、分），某个时间整点自动执行检查。被清理的数据，可以在清理列表中查看，并可对已经清理的数据进行恢复。
4. 单击**保存**，完成数据自动清理任务的设置。

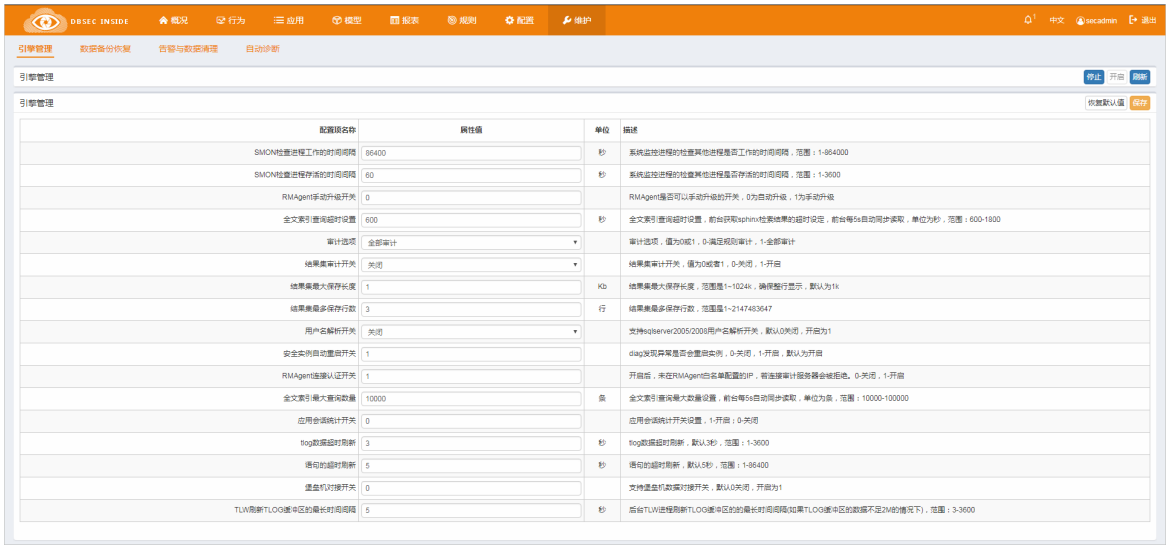
   被清理的数据，可以在清理列表中查看，并可对已经清理的数据进行恢复。

10.3.4.7.3. 引擎管理

该章节介绍如何管理数据库审计的引擎。

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. 单击**维护 > 引擎管理**。



3. 在**引擎管理**页面，您可对数据库引擎执行以下操作，对引擎进行管理。
   - 单击**开启**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。

10.3.5. 审计管理员指南

10.3.5.1. 查看系统操作日志

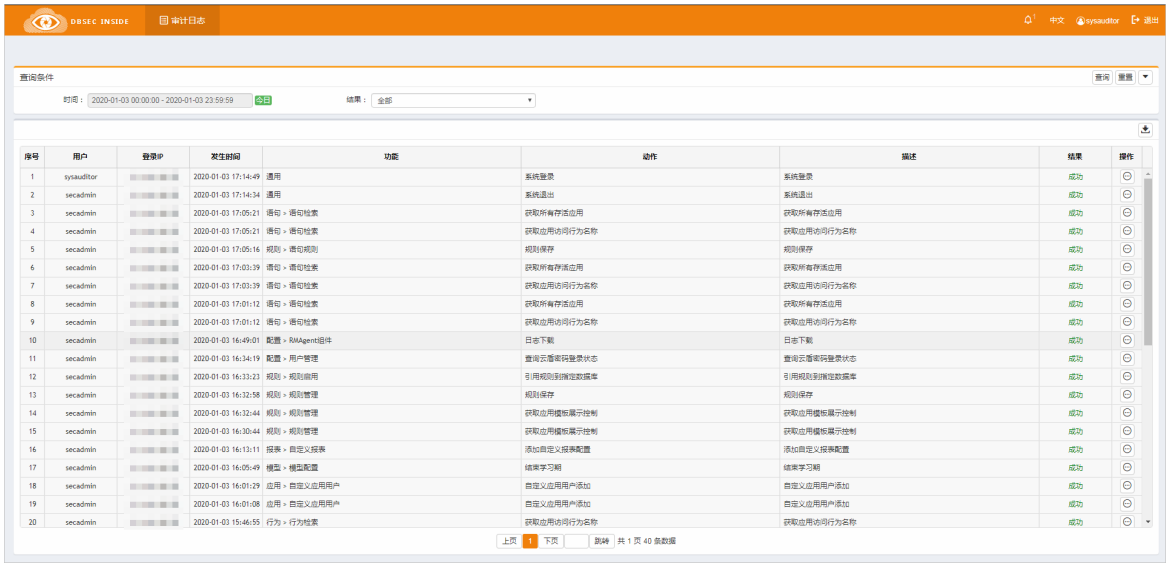
该章节介绍如何查看系统的操作日志。

背景信息

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。

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。
2. 在**审计日志**页面，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。



单击日志记录列表右上角的导出报告按钮，可将当前列表中的审计日志记录导出到本地。

3. 单击某一审计日志操作栏中的详细按钮，可以查看该审计日志的详细信息。



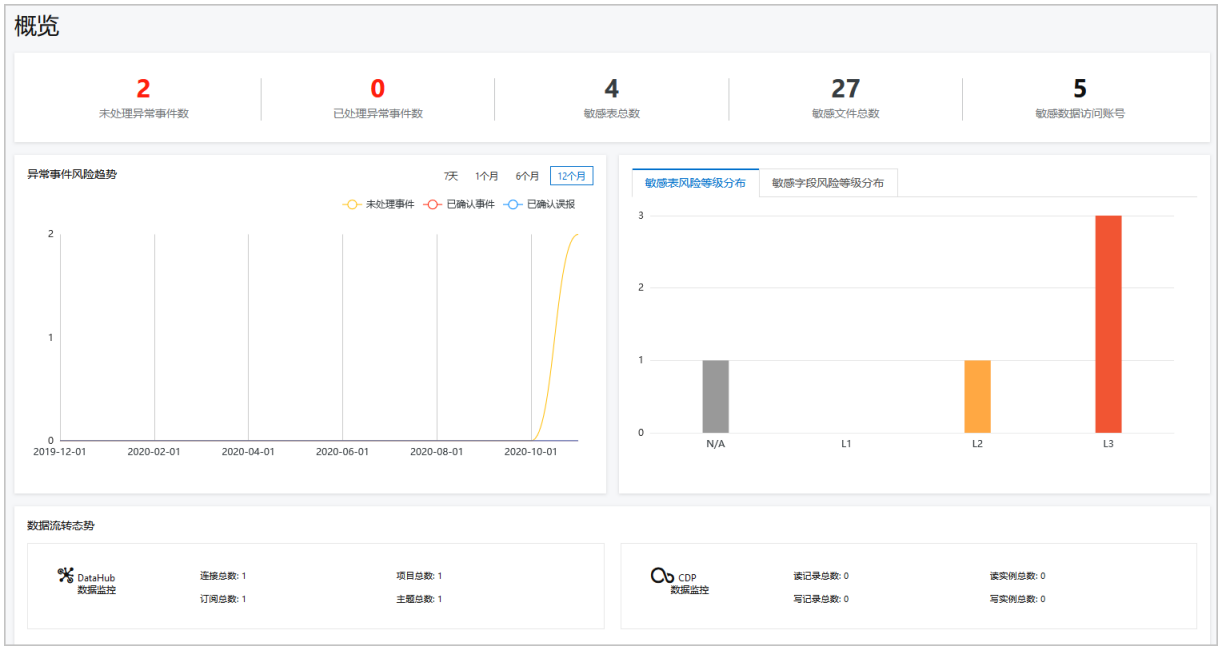
10.4. 敏感数据保护

10.4.1. 敏感数据保护概览

本文介绍敏感数据保护的整体信息。通过对敏感数据保护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的敏感数据安全情况。

敏感数据保护（Sensitive Data Discovery and Protection，简称SDDP）可以从您资产的海量数据中快速发现和定位敏感数据，追踪敏感数据的使用情况，并根据您选择的安全管理规则，为您呈现系统化的数据总览图，以确保您能实时了解资产数据的安全状态。

在**数据安全 > 敏感数据保护 > 概览**页面，查看敏感数据保护整体情况。



- **概览**：整体展现敏感数据的信息，包括**未处理异常事件数**、**已处理异常事件数**、**敏感表总数**、**敏感文件总数**和**敏感数据访问账号**。

- **异常事件风险趋势**：图形化展示异常事件的趋势，可选择**7天**、**1个月**、**6个月**、**12个月**等时间段，支持查看**未处理事件**、**已确认事件**、**已确认误报**等趋势曲线。
- **敏感表风险等级分布**：展示敏感表S3（高敏感）、S2（中敏感）、S1（低敏感）和N/A（未识别敏感）各风险等级的分布。
- **敏感字段风险等级分布**：展示敏感字段S3（高敏感）、S2（中敏感）、S1（低敏感）和N/A（未识别敏感）各风险等级的分布。
- **数据流转态势**：
  - 展示Datahub、CDP两种数据流转产品的核心流转数据动态统计。
  - 实现可视化动态数据流转图，流转图能动态展示数据流转情况和异常产出情况，并能通过流转图中异常位置直接重定向到**数据流转异常**处理页面。

    支持在大数据环境下，数据存储产品MaxCompute、ADS、OSS、OTS等；数据传输产品Datahub、CDP；数据流处理产品Blink；外部数据库；外部文件等实体的数据链路监控。

10.4.2. 数据资产授权

10.4.2.1. 数据资产授权

敏感数据保护服务SDDP在检测数据源（OSS、RDS、DRDS、表格存储OTS、ECS自建数据库、MaxCompute、ADS、OceanDB、GPDB）中存储的敏感数据之前，需要首先获取允许访问这几类产品中指定数据的授权。本文介绍数据资产授权的操作步骤。

背景信息

资产保护授权功能允许SDDP访问具体产品中存有数据的部分空间或项目。如果不授权，SDDP将无法对产品中的敏感数据进行识别和脱敏。

> **注意** 已开启授权的OSS Bucket（OSS文件桶）会消耗您的OSS存储容量，已开启授权的数据库或项目会消耗您的数据库和项目数。只有在OSS存储容量、数据库和项目数量充足时，您才可以成功进行相应授权操作。您可以在**云上托管**页面查看剩余的OSS存储容量、数据库和项目数。

SDDP支持授权的数据源如下所示：

- OSS文件桶授权方法，请参见OSS文件桶访问授权。
- RDS库授权方法，请参见RDS库访问授权。
- DRDS授权方法，请参见DRDS访问授权。
- OTS授权方法，请参见OTS访问授权。
- ECS自建数据库授权方法，请参见自建数据库访问授权。
- MaxCompute项目授权方法，请参见MaxCompute项目访问授权。
- ADS授权方法，请参见ADB访问授权。
- OceanBase授权方法，请参见OceanBase访问授权。

OSS文件桶访问授权

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**OSS**页签下，为Bucket授权。

- 如只需为一个Bucket授权，可以在Bucket所在行单击**识别权限**、**脱敏权限**、**OCR权限**、**审计权限**开关来开启或关闭权限，设置**敏感数据采样**、**审计日志存档**。

参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
OCR权限	开启或关闭SDDP对图片中的文本进行敏感数据识别的权限。
审计权限	开启或关闭SDDP对选中资产进行数据审计的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行深入判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。 **说明** 设置审计日志存档时间无需您额外开通日志服务。

- 如需为多个Bucket授权，执行以下操作对各Bucket批量设置权限。
  a. 选中需要授权的Bucket，单击**批量操作**。

b. 在**对于选中资产批量处理**对话框中，设置识别权限、审计权限、脱敏权限、OCR权限等参数。



c. 单击**确认**。

完成资产授权后，SDDP将会对开启授权的OSS存储空间中的文件执行敏感数据检测。如果该存储空间是首次开启授权，SDDP将会自动触发全量扫描。

已授权资产可进行编辑或取消授权。取消授权后，SDDP不会检测该文件桶中的数据。

> 说明 SDDP仅对已授权的Bucket进行数据扫描和风险分析。

RDS库访问授权

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**RDS**页签。
5. 在**RDS**页签，单击**未授权**。
6. 定位到需要授权的实例，在**用户名**和**密码**文本框输入连接数据库的用户名和密码。

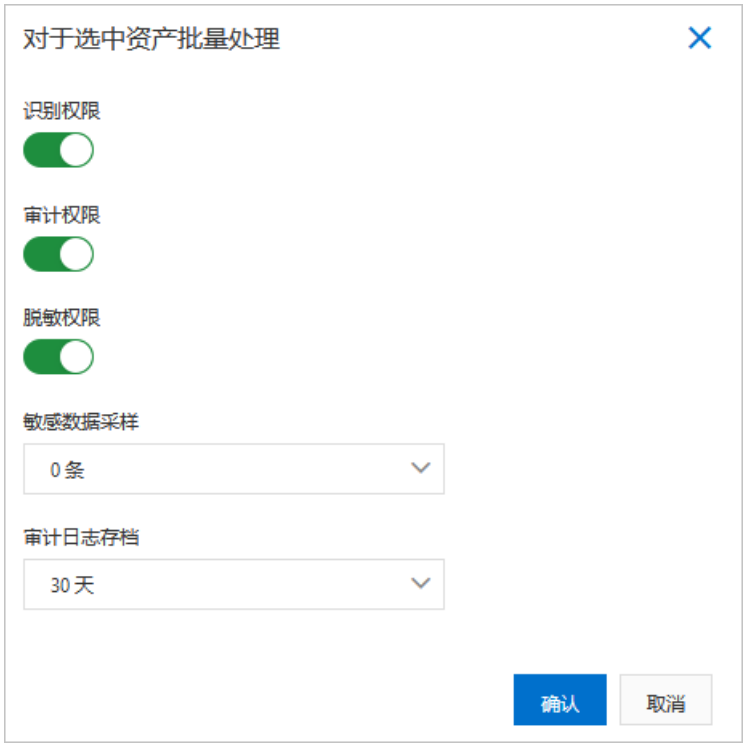
   您可以使用SDDP提供的**批量密码导入**功能，批量导入数据库的用户名和密码。更多信息，请参见批量密码导入。

   > 注意 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

7. 选中需要授权的资产，单击**批量操作**。

您也可以单击某个实例操作列下的**一键授权**为该实例授权。

8. 在授权页面，设置识别权限、审计权限、脱敏权限等参数。



参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
审计权限	开启或关闭SDDP对选中资产中进行数据审计的权限。 SDDP支持审计日志功能，审计日志数据提供了包括审计规则命中结果、审计规则检测的资产类型、命中规则的操作类型和操作账号等信息，覆盖资产数据产生、更新和使用等全链路的日志数据。 SDDP安全审计功能的使用，请参见审计规则。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

9. 单击**确认**。

> **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，SDDP会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该RDS数据库合法用户的用户名和密码。取消授权后，SDDP不会检测该数据库中的数据。

DRDS访问授权

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**DRDS**页签。
5. 在**DRDS**页签，单击**未授权**。
6. 定位到需要授权的实例，在**用户名**和**密码**文本框输入连接数据库的用户名和密码。

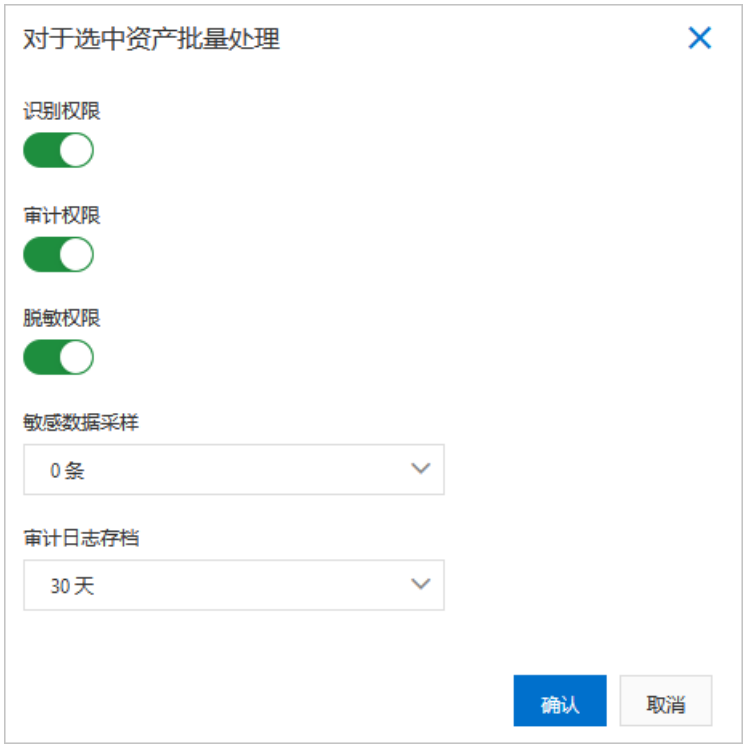
   您可以使用SDDP提供的**批量密码导入**功能，批量导入数据库的用户名和密码。更多信息，请参见批量密码导入。

   > 注意 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

7. 选中需要授权的资产，单击**批量操作**。

   您也可以单击某个实例操作列下的**一键授权**为该实例授权。

8. 在授权页面，设置识别权限、审计权限、脱敏权限等参数。



参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。

参数	说明
审计权限	开启或关闭SDDP对选中资产中进行数据审计的权限。 SDDP支持审计日志功能，审计日志数据提供了包括审计规则命中结果、审计规则检测的资产类型、命中规则的操作类型和操作账号等信息，覆盖资产数据产生、更新和使用等全链路的日志数据。 SDDP安全审计功能的使用，请参见审计规则。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

9. 单击**确认**。

> **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，SDDP会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该DRDS数据库合法用户的用户名和密码。取消授权后，SDDP不会检测该数据库中的数据。

OTS访问授权

OTS即表格存储服务。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**OTS**页签。
5. 在**OST**页签下，为实例或Bucket授权。
   - 如只需为一个实例或Bucket授权，可以在实例或Bucket所在行单击**识别权限**、**脱敏权限**、**审计权限**开关来开启或关闭权限，设置**敏感数据采样**、**审计日志存档**。

参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
审计权限	开启或关闭SDDP对选中资产进行数据审计的权限。

参数	说明
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

- 如需为多个实例或Bucket授权，执行以下操作对各实例或Bucket批量设置权限。
  a. 选中需要授权的实例或Bucket，单击**批量操作**。
  b. 在**对于选中资产批量处理**对话框中，设置识别权限、审计权限、脱敏权限等参数。
  c. 单击**确认**。

授权完成后，SDDP会检测该资产中的敏感数据。

自建数据库访问授权

SDDP支持检测的ECS自建数据库有以下限制：

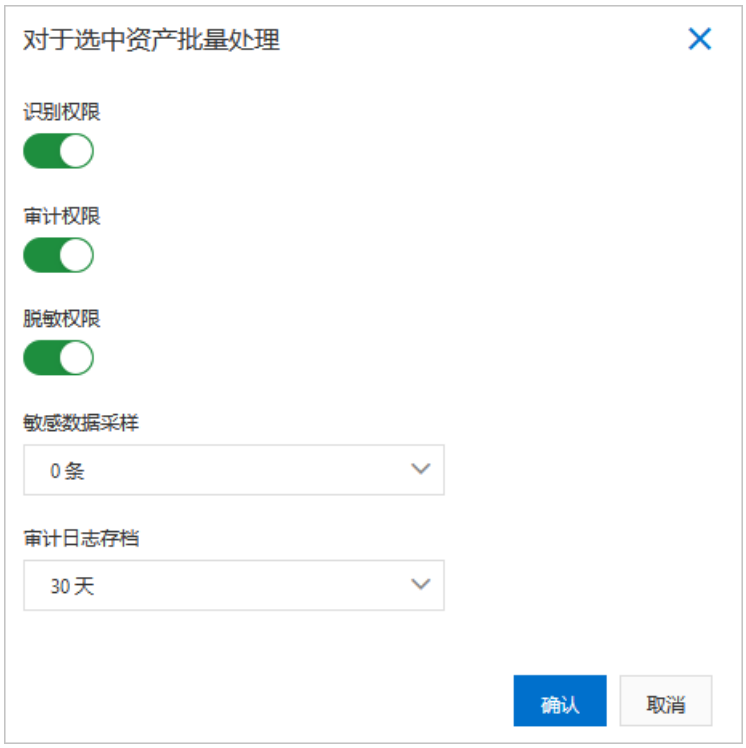
- 仅VPC网络中的ECS自建数据库支持使用SDDP服务。
- 目前支持MySQL、SQL Server、Oracle三种类型的ECS自建数据库。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**ECS自建数据库**页签。
5. 在**自建数据库**页签，单击**添加数据资产**。
6. 在**资产授权**对话框中，配置相应参数并单击**下一步**。
   您可以参考以下表格中的参数说明配置相应参数。

参数	说明
区域	选择您需要授权SDDP访问的ECS自建数据库的所在区域。
ECS实例ID	选择您需要授权SDDP访问的ECS自建数据库所在的ECS实例ID。
数据库类型	选择您需要授权SDDP访问的ECS自建数据库的类型。 目前SDDP支持MySQL、SQL Server、Oracle三种类型的ECS自建数据库。
库名称	输入您需要授权SDDP访问的ECS自建数据库名称。 **说明** 如果当前ECS实例下还有其他ECS自建数据库需要授权SDDP访问，您可以单击**添加数据库**，填写其他ECS自建数据库的信息。

参数	说明
端口	填写访问ECS自建数据库使用的端口号。
用户名	输入可以访问ECS自建数据库合法用户的用户名。
密码	输入可以访问ECS自建数据库合法用户的密码。

7. 在授权页面，设置识别权限、审计权限、脱敏权限等参数。



参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
审计权限	开启或关闭SDDP对选中资产中进行数据审计的权限。 SDDP支持审计日志功能，审计日志数据提供了包括审计规则命中结果、审计规则检测的资产类型、命中规则的操作类型和操作账号等信息，覆盖资产数据产生、更新和使用等全链路的日志数据。 SDDP安全审计功能的使用，请参见审计规则。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。

参数	说明
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

8. 单击**确定**。
   授权完成后，SDDP会检测该资产中的敏感数据。

MaxCompute项目访问授权

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**MaxCompute**页签。
5. 在**MaxCompute**页签下，为实例或Bucket授权。
   - 如只需为一个实例或Bucket授权，可以在实例或Bucket所在行单击**识别权限**、**脱敏权限**、**审计权限**开关来开启或关闭权限，设置**敏感数据采样**、**审计日志存档**。

参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
审计权限	开启或关闭SDDP对选中资产进行数据审计的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

   - 如需为多个实例或Bucket授权，执行以下操作对各实例或Bucket批量设置权限。
     a. 选中需要授权的实例或Bucket，单击**批量操作**。
     b. 在**对于选中资产批量处理**对话框中，设置识别权限、审计权限、脱敏权限等参数。
6. 单击**确认**。

   > **说明** 若授权未通过，请检查授权参数是否有误或SDDP访问子账号是否添加成功。

   授权完成后，SDDP会对该项目列表中的所有数据进行检测。

   资产完成授权后可取消授权。取消授权后，SDDP不会检测该资产中的数据。

ADB访问授权

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**ADB-MYSQL**或**ADB-PG**页签。
5. 在对应页签，单击**添加数据资产**。
6. 在**添加数据资产**对话框中，配置相应参数并单击**确认**。

   您可以参考以下表格中的参数说明配置相应参数。

参数	说明
所在区域	选择您需要授权SDDP访问的ADS数据库的所在区域。
实例名称	选择您需要授权SDDP访问的ADS数据库的实例名称。
数据库名称	输入您需要授权SDDP访问的ADS数据库的名称。
用户名	输入可以访问ADS数据库合法用户的用户名和密码。
密码	
自动扫描	开启该功能后，每次修改识别规则配置，会自动触发针对该资产的重新扫描。

7. 在页签下，为实例或Bucket授权。
   - 如只需为一个实例或Bucket授权，可以在实例或Bucket所在行单击**识别权限**、**脱敏权限**、**审计权限**开关来开启或关闭权限，设置**敏感数据采样**、**审计日志存档**。

参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
审计权限	开启或关闭SDDP对选中资产进行数据审计的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

   - 如需为多个实例或Bucket授权，执行以下操作对各实例或Bucket批量设置权限。
     a. 选中需要授权的实例或Bucket，单击**批量操作**。
     b. 在**对于选中资产批量处理**对话框中，设置识别权限、审计权限、脱敏权限等参数。
     c. 单击**确认**。

授权完成后，SDDP会检测该资产中的敏感数据。

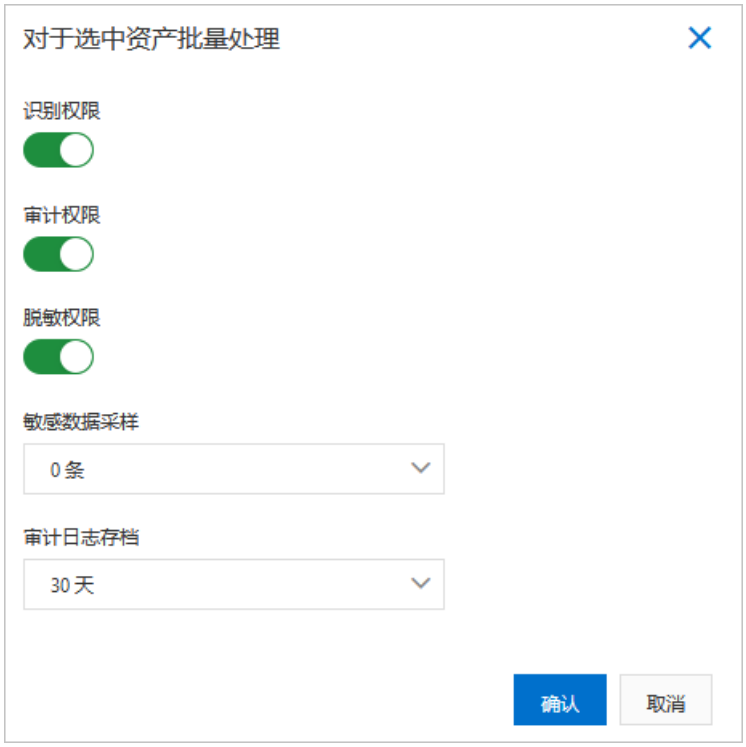
OceanBase访问授权

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面，单击**OceanBase**页签。
5. 在**OceanBase**页签，单击**添加数据资产**。
6. 在**资产授权**对话框中，配置相应参数并单击**下一步**。

   您可以参考以下表格中的参数说明配置相应参数。

参数	说明
区域	选择您需要授权SDDP访问的OceanBase数据库的所在区域。
数据库类型	选择您需要授权SDDP访问的OceanBase数据库的类型。 目前SDDP仅支持MySQL和Oracle两种类型的OceanBase数据库。
集群名称	选择您需要授权SDDP访问的OceanBase数据库的所在集群名称。
租户名称	选择您需要授权SDDP访问的OceanBase数据库所属租户名称。
数据库名称	输入您需要授权SDDP访问的OceanBase数据库名称。 **说明** 如果当前ECS实例下还有其他OceanBase数据库需要授权SDDP访问，您可以单击**添加数据库**，填写其他OceanBase数据库的信息。
链接地址	填写访问OceanBase数据库使用的链接地址。
用户名	输入可以访问OceanBase数据库合法用户的用户名和密码。
密码	

7. 在授权页面，设置识别权限、审计权限、脱敏权限等参数。



参数	说明
识别权限	开启或关闭SDDP识别选中资产敏感数据的权限。
审计权限	开启或关闭SDDP对选中资产中进行数据审计的权限。 SDDP支持审计日志功能，审计日志数据提供了包括审计规则命中结果、审计规则检测的资产类型、命中规则的操作类型和操作账号等信息，覆盖资产数据产生、更新和使用等全链路的日志数据。 SDDP安全审计功能的使用，请参见审计规则。
脱敏权限	开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
敏感数据采样	当开启**识别权限**开关时，需要设置SDDP对选中资产进行敏感数据采样的条数。 敏感数据采样是指SDDP自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入地判断。 可选取值包括**0条**、**5条**、**10条**。
审计日志存档	当开启**审计权限**开关时，需要设置选中资产的审计日志保存时间。 可选取值包括**30天**、**90天**、**180天**。

8. 单击**确定**。
   授权完成后，SDDP会检测该资产中的敏感数据。

批量密码导入

SDDP支持通过Excel模板批量导入RDS、DRDS和ECS自建数据库未授权数据库的用户名和密码，方便您批量授权SDDP访问多个数据库项目。以下介绍批量导入数据库密码的详细步骤。

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
4. 在**云上托管**页面右上角，单击**批量密码导入**。
5. 在**批量密码导入**对话框中，单击**SDDP授权文件模板.xlsx**。
6. 打开下载到本地的模板文件，编辑数据库产品中的**用户名**和**密码**列并保存模板文件。

   如果您修改了模板文件中已有的用户名和密码，批量导入密码操作完成后，已有的用户名和密码将被更新为您修改后的用户名和密码。
7. 在**批量密码导入**对话框中，单击**文件上传**，完成修改后模板的上传。
8. 单击**确定**。
   Excel文件成功上传后，SDDP会自动为您在**RDS**、**DRDS**和**ECS自建数据库**页签下的**用户名**和**密码**列导入该Excel文件中的数据库用户名和密码。您无需手动填写数据库的用户名和密码，即可在**云上托管**页面执行批量授权操作，对多个数据库进行批量SDDP访问授权。

10.4.2.2. 授权账密管理

为确保敏感数据保护服务SDDP能正常获取检测数据源中存储敏感数据的权限，需要正确配置连接数据库的用户名和密码。本文介绍如何查看、添加连接数据库的用户名、密码。

背景信息

目前，SDDP支持管理RDS、DRDS的授权账密。

查看授权账密

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 授权账密管理**。
4. 在页签中，选择目标数据源（例如**RDS**）。



5. （可选）设置搜索项，搜索目标实例。

   > **说明** 如果需要查看全部实例信息，可忽略此步骤。

搜索项	说明
区域	选择您需要搜索的数据库所在区域。
实例/Bucket	选择您需要搜索的实例或Bucket名称。
数据库类型	选择您需要搜索的数据库类型。 RDS、DRDS可搜索MySQL和SQL Server数据库。

6. 在实例列表中查看数据库及账密信息。

添加授权账密

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据保护授权 > 授权账密管理**。
4. 在页签中，选择目标数据源（例如RDS）。



5. 定位到需要添加账密的实例，在**用户名**和**密码**文本框输入连接数据库的用户名和密码。

> 注意 用户名和密码错误将会导致SDDP数据资产授权失败，请您输入正确的用户名和密码。

6. 单击**添加**。
   数据库的用户名、密码添加成功后，实例对应的**状态**显示**添加成功**。

后续步骤

如需更新数据库的用户名、密码，可单击目标实例**操作**列的**编辑**。

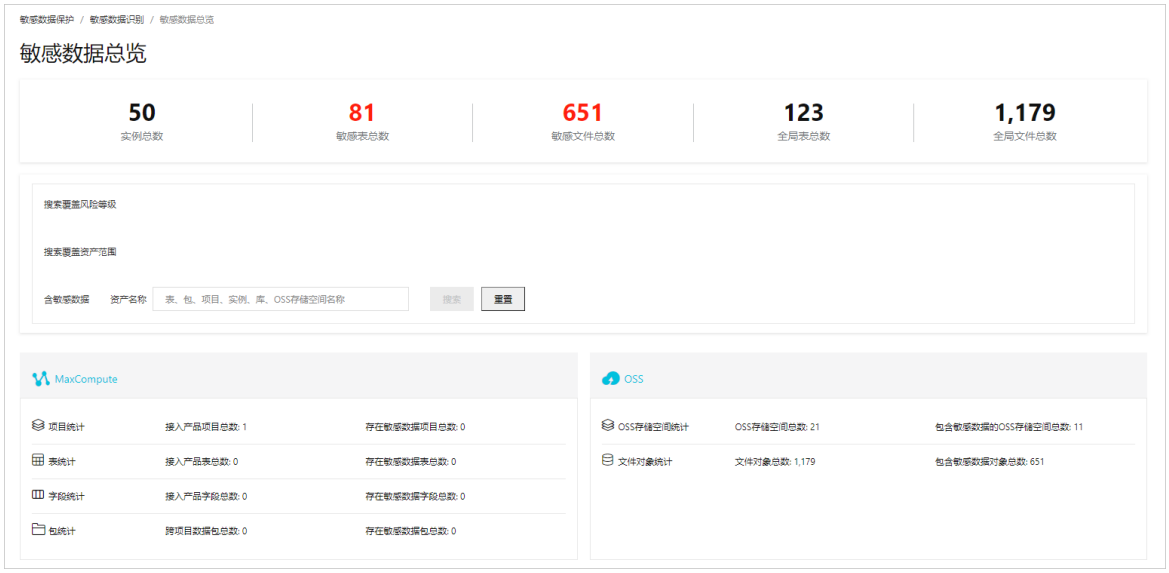
修改后，单击**保存**。

10.4.3. 敏感数据发现

10.4.3.1. 敏感数据总览

本文介绍数据资产的总体情况。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据识别 > 敏感数据总览**。
4. 在**敏感数据总览**页面，查看敏感数据保护整体情况。



- 整体敏感数据信息：展示**敏感实例总数**、**敏感表总数**、**敏感文件总数**、**全局表总数**、**全局文件总数**。
- 敏感数据搜索：通过风险等级、资产范围、敏感数据类型、资产名称等信息，搜索敏感数据。
- 实时统计和展示MaxCompute、OSS、ADS、OTS等产品的接入情况和敏感数据情况。

10.4.3.2. 查看敏感数据资产

SDDP支持检测OSS、RDS、MaxCompute等数据源中的敏感数据。本文介绍如何查看SDDP在OSS、RDS、MaxCompute等数据源中检测出的敏感数据。

查看OSS敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**OSS**页签下，定位到需要查看详情的Bucket，单击其操作列下的**文件详情**。
5. 在**OSS对象查询**面板，您可以查看敏感文件占比、命中规则TOP 5和存在敏感数据的文件列表。
   - **查看敏感文件占比**

     在**敏感文件占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的文件的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的文件列表**

     在文件列表区域，您可以查看存在敏感数据的文件的名称、大小、类型和敏感字段数等信息。单击操作列下的**命中详情**，可以查看当前文件命中的敏感数据检测规则的详细信息。

查看RDS敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。

4. 在**敏感数据资产**页面，单击RDS页签。
5. 在RDS页签下，定位到需要查看详情的RDS实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看MaxCompute敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击MaxCompute页签。
5. 在MaxCompute页签下，定位到需要查看详情的MaxCompute实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看ECS自建数据库敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击**ECS自建数据库**页签。
5. 在**ECS自建数据库**页签下，定位到需要查看详情的数据库实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **查看存在敏感数据的表**

  在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看DRDS敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击**DRDS**页签。
5. 在**DRDS**页签下，定位到需要查看详情的数据库实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看OTS敏感数据

OTS即表格存储服务。

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击**OTS**页签。
5. 在**OTS**页签下，定位到需要查看详情的实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看ADB-PG敏感数据

1.

2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击**ADB-PG**页签。
5. 在**ADB-PG**页签下，定位到需要查看详情的实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看ADB-MYSQL敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击**ADB-MYSQL**页签。
5. 在**ADB-MYSQL**页签下，定位到需要查看详情的实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。
   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。
   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看DataWorks敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击**DataWorks**页签。
5. 在**DataWorks**页签下，定位到需要查看详情的实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。

- **查看命中规则Top 5**

  在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **查看存在敏感数据的表**

  在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

查看OceanBase敏感数据

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**敏感数据识别 > 敏感数据资产**。
4. 在**敏感数据资产**页面，单击OceanBase页签。
5. 在OceanBase页签下，定位到需要查看详情的实例，单击其操作列下的**表详情**。
6. 在**表查询**面板，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。
   - **查看敏感表占比**

     在**敏感表占比**区域，您可以查看L3（高敏感）、L2（中敏感）、H1（低敏感）和N/A（未识别敏感）程度的表的数量和占比饼状图。

   - **查看命中规则Top 5**

     在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

   - **查看存在敏感数据的表**

     在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。单击操作列下的**列详情**，可以查看命中敏感数据规则的列、敏感等级等详细信息。

10.4.3.3. 搜索敏感数据

敏感数据搜索页面为您展示了资产中的所有敏感数据，您可以输入敏感数据或敏感数据的组合作为搜索条件，快速定位所关注的敏感数据在所有资产中的分布情况。本文介绍如何搜索敏感数据。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据识别 > 敏感数据搜索**。
4. 在**敏感数据搜索**页面，设置搜索条件。



您可以设置以下搜索条件：

- **命中数据**：选择需要查看的敏感数据类型，支持同时选择多个类型。例如：同时选择手机号和邮箱。
- **输入文件名称**或**输入表名称**：输入需要查看敏感数据的文件名称或表名称。文件名称和表名称都支持模糊搜索。
- **区域**：选择需要查看的数据源实例所在地域。
- **Bucket、实例或项目**：选择需要搜索的Bucket、实例或项目名称。

> **说明** 如果您同时设置了多个搜索条件，将为您展示同时满足这些搜索条件的敏感数据列表。

5. 单击**搜索**。

   在**敏感数据搜索**的列表中，可以查看搜索出的敏感数据所在文件或表信息。文件或表信息可以通过以下方式进行筛选或排序：

   - **按敏感等级搜索**

     在**OSS-文件**页签下的搜索结果中，设置**敏感等级**（S1、S2、S3）查看指定敏感等级的敏感数据列表。

   - **按总行数或敏感列数量升序或降序排敏感数据**

     在**RDS-表**页签等产品的敏感数据搜索结果下，单击**总行数**或**敏感列**右侧的图标，按照表总行数或敏感列数量升序或降序排列当前列表中的敏感数据。单击第一次为降序排列，第二次切换到升序排列。



6. 定位到具体的敏感数据列，单击目标文件**操作**列的**详情**或单击目标表**操作**列的**列详情**。

   在Bucket的**命中查询**或表的**列详情**面板，可以查看当前文件或表中检测出的所有敏感数据的详细信息，包括以下内容：

   - **列名称**：命中敏感数据的列名称。

     > **说明** RDS、MaxCompute、ECS自建数据库、DRDS、OTS、ADS和GPDB的**列详情**面板会展示该参数。OSS文件的**命中查询**面板不会展示该参数。

   - **命中规则**：命中敏感数据的规则分类和规则名称。
   - **敏感等级**：敏感数据的等级。
   - **命中数量**：当前规则在该文件中命中敏感数据的次数。

     > **说明** OSS文件的**命中查询**面板会展示该参数。

   - **数据采样**：展示SDDP识别的敏感数据字段。您可以选择**数据安全 > 敏感数据保护 > 数据保护授权 > 数据资产授权**，在**云上托管**页面设置**敏感数据采样**的数量，可以设置为0条、5条或10条。此处显示的采样数据个数与您资产保护授权时**敏感数据采样**设置的数值保持一致。

10.4.3.4. 识别任务监控

SDDP自动为识别权限授权成功的资产创建敏感数据扫描任务。您可以在识别任务监控页面，查看敏感数据扫描任务的详细信息、执行重新扫描操作。

背景信息

SDDP支持监控OSS、RDS、MaxCompute、ECS自建数据库、DRDS、OTS（即表格存储）、OceanBase、ADB-MYSQL和ADB-PG的敏感数据扫描任务。

数据源授权成功后，SDDP自动为该产品的相应资产创建扫描任务并立即执行敏感数据检测。SDDP创建扫描任务后会默认开启**自动扫描**。开启自动扫描服务后，自动进行首次扫描，之后每隔4个小时重新扫描资产中新增或修改的数据。新增或修改识别规则都会触发扫描任务。

查看扫描任务详细信息

您可以在**识别任务监控**页面查看敏感数据检测任务相关的资产、扫描状态和完成时间等信息。以下步骤介绍如何查看扫描任务的详细信息。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据识别 > 识别任务监控**
4. 选择需要查看的数据源，并单击其页签。
5. （可选）在搜索栏，您可以输入实例或Bucket名称，选择区域、起始时间和结束时间，并单击**搜索**查看指定任务。
6. 在任务列表，您可以查看扫描任务相关的资产、Bucket名称、扫描时间、扫描状态和完成时间等信息。

重新扫描资产

以下是重新扫描资产的应用场景说明：

- 未开启**自动扫描**的任务，需要您执行重扫操作才会进行敏感数据扫描。
- 已开启**自动扫描**的任务，默认每4个小时扫描资产中新增或修改的数据。如果您修改了服务器数据需要立即扫描资产中是否存在敏感数据，您可以进行重扫操作。

以下步骤介绍如何重新扫描资产中的敏感数据。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 选择需要重新扫描资产的数据源，并单击其页签。
4. 定位到需要重新扫描的实例，并单击其**操作**列下的**重扫**。
5. 在**确定重新扫描**对话框中，单击**确定**。

   一般情况下，重新扫描可以在10分钟以内完成，请您耐心等待。

   开始重新扫描后，扫描状态将变为**扫描中**或**等待**。您可以在**扫描状态**列查看扫描进度。

后续步骤

扫描完成后，扫描状态将变为**完成**。您可以到**数据安全 > 敏感数据保护 > 敏感数据识别 > 敏感数据资产**对应数据源页签，查看最新扫描结果。

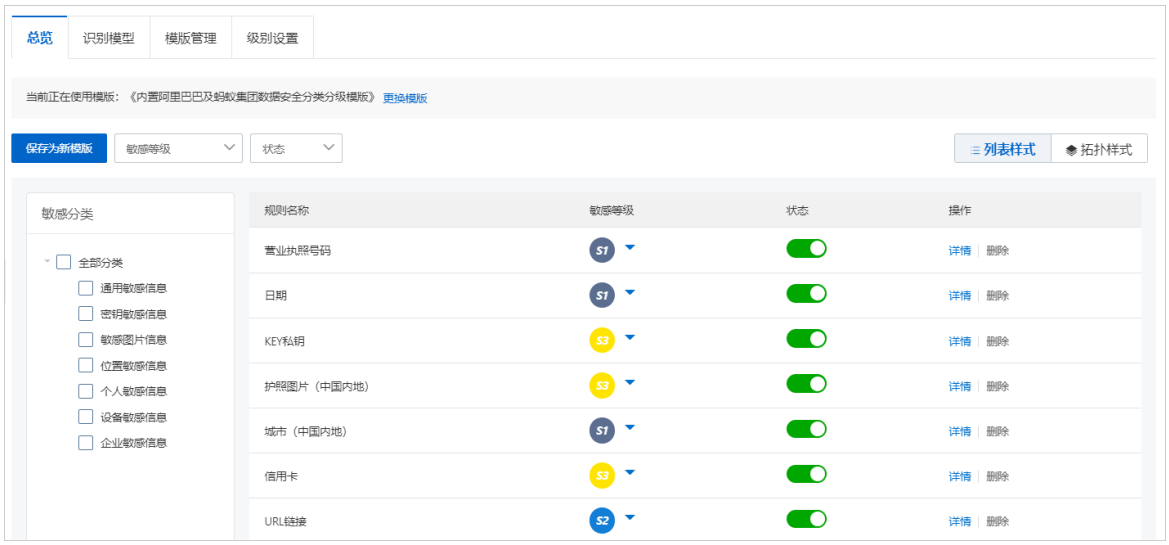
10.4.3.5. 识别规则

10.4.3.5.1. 查看识别规则

敏感数据保护SDDP支持自定义敏感信息的分级规则，本文介绍如何查看敏感数据识别规则的总览。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据发现 > 识别规则**，在**识别规则**页面单击**总览**页签。
4. 在**总览**页签，通过设置**敏感等级**、**状态**，查看当前使用模板中符合设置条件的规则信息。

   您可以单击**列表样式**或**拓扑样式**，选择规则的显示样式。您还可以通过选择**敏感分类**栏目的敏感类型，筛选规则。



   在**总览**页面，您还可以进行如下操作：

   - 更换模板：单击**更换模板**，可以跳转至**模板管理**页签，便于模板切换。
   - 保存新模板：单击总览页面左上方的**保存为新模板**，可以将显示的识别规则保存为一个新模板，显示在**模板管理**页签。
   - 修改规则状态：通过开启或关闭指定规则**状态**列的开关，开启或关闭规则，识别的时候识别开启的规则。
   - 查看规则详情：单击指定规则**操作**列的**详情**，您可以查看该规则的详细信息，并且可以进行修改。
   - 删除规则：单击指定规则**操作**列的**删除**，您可以删除此条规则。

10.4.3.5.2. 管理识别模型

识别模型定义了识别您资产中敏感数据的具体规则。识别模型包含识别典型敏感数据的内置识别模型和自定义识别模型。本文介绍如何查看内置识别模型、添加、编辑和删除自定义识别模型。

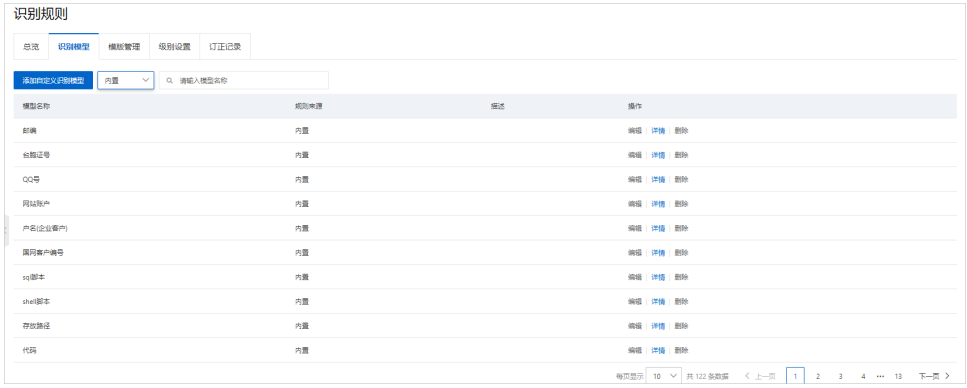
查看内置识别模型

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据发现 > 识别规则**。
4. 在**识别规则**页面，单击**识别模型**页签。
5. 设置搜索条件**规则来源**为**内置**。



6. 查看内置识别模型列表。

   您可以查看内置识别模型的名称等信息。

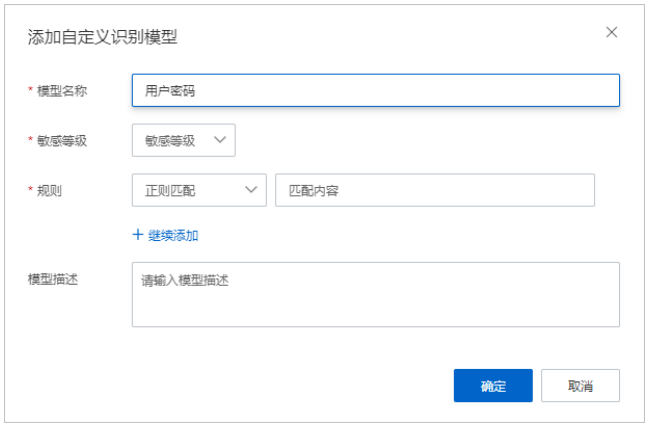


7. 单击指定内置规则**操作**列下的**详情**，查看该内置识别模型的信息。

> 说明 内置识别模型不支持修改和删除。

添加自定义识别模型

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据发现 > 识别规则**。
4. 在**识别规则**页面，单击**识别模型**页签。
5. 在**识别模型**页签下，单击**添加自定义识别模型**。
6. 在**添加自定义识别模型**对话框，配置以下参数。



参数	说明
模型名称	输入识别模型的名称。
敏感等级	选择识别模型识别出的敏感数据对应的风险等级。 风险等级包括： ○ **S1**：一级敏感数据 ○ **S2**：二级敏感数据 ○ **S3**：三级敏感数据 ○ **S4**：四级敏感数据 ○ **S5**：五级敏感数据
规则	设置敏感数据的识别规则。可选： ○ **不包含**：使用不包含某个关键字来定义敏感数据识别规则。 ○ **包含**：使用包含某个关键字来定义敏感数据识别规则。 ○ **正则匹配**：使用正则表达式来定义敏感数据识别规则。可参考以下示例配置该参数： ■ *Exampleoo+a*：表示Exampleooa、Exampleoooa、Exampleooooooa等都会被识别为敏感数据。*+*表示该符号前面的字符必须至少出现一次。 ■ *Exampleoo*a*：表示Exampleoa、Exampleooa、Exampleooooooa等都会被识别为敏感数据。*表示该符号前面的字符可以不出现，也可以出现一次或多次。 ■ *Exampleo?a*：表示只有Examplea、Exampleoa会被识别为敏感数据。*?* 表示该符号前面的字符可以不出现或最多出现一次。 一个规则模型中可以添加多条规则。需要设置多条规则时，您可以单击**继续添加**在当前识别模型下再添加一条识别规则。
模型描述	输入识别模型的描述信息。

7. 单击**确定**。
   创建完成后，您可以在识别模型列表中查看新创建的识别模型。



查看、编辑、删除自定义识别模型

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据发现 > 识别规则**。
4. 在**识别规则**页面，单击**识别模型**页签。
5. 将搜索条件**规则来源**设置为**自定义**。

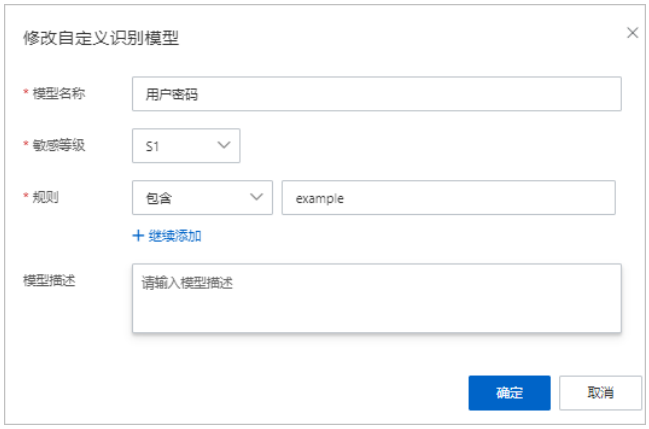
6. 定位到待操作的识别模型，执行以下操作。
   - **查看自定义识别模型详情**

     需要查看某个自定义识别模型的详情时，单击该识别模型操作列下的**详情**，在**查看自定义识别模型**对话框，查看该识别模型的详情。



   - **编辑自定义识别模型**

     需要修改某个自定义识别模型的敏感数据识别规则时，单击该识别模型操作列下的**编辑**，在**修改自定义识别模型**对话框中，修改该识别模型的参数，并单击**确定**。



   - **删除自定义识别模型**

     不再需要使用某个自定义识别模型时，单击该识别模型**操作**列下的**删除**，在确认对话框单击**确定**。

10.4.3.5.3. 管理模板

本文介绍了如何启用、查看、复制模板。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据识别 > 识别规则**，单击**模版管理**页签。
4. 在**模版管理**页签，查看可用模板。



- 启用模板：单击指定模板的**启用**，您可以切换至该模板。由于更换模板会重新扫描全部数据，限定10分钟内模板仅能更换一次。
- 查看模板详情：单击指定模板的**详情**，您可以查看具体的分类。



- 复制模板：单击指定模板的**复制**，您可以复制该模板生成一个同样的模板。

10.4.3.5.4. 设置风险级别

本文介绍如何设置敏感数据的风险级别。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据识别 > 识别规则**，单击**级别设置**页签。
4. 在**级别设置**页签，单击**添加分级**，设置**敏感级别**和级别的描述。

   SDDP默认提供了**N/A**和S1~S10的十一种风险级别，**N/A**表示敏感等级未知的数据，S1~S10风险等级对应的危害程度依次递增。您可以设置这十一个等级的描述，帮助您更好地对您资产中的敏感数据进行分

类。

5. 定位到需要编辑的风险级别，单击**操作**列的**编辑**。
6. 在**编辑分级**对话框，修改级别描述。
7. 单击**确认**。

10.4.4. 云原生数据审计

10.4.4.1. 审计概览

审计概览页面从审计告警总览、资产管理和安全保障、审计告警和泄漏风险、安全性变化角度向您展示了您资产中存在的敏感信息的统计数据。本文介绍了审计概览页面展示的不同数据内容，帮助您更好地了解资产中存在的敏感数据。

背景信息

智能审计每日自动更新审计报表，并为您展示上一周的报表统计数据。

访问审计报表页面

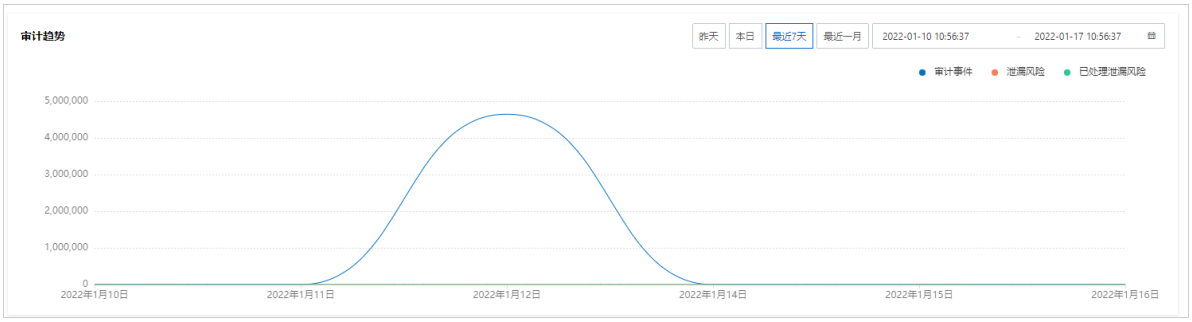
1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**云原生数据审计 > 审计概览**，在**审计概览**页面您可以查看以下模块的内容。
   - 审计告警总览
   - 资产管理和安全保障
   - 审计告警和泄漏风险
   - 安全性变化

     审计报表左上角展示了审计报表统计的时间范围。您可以设置**昨天**、**本日**、**最近7天**、**最近一月**、自定义查看审计概览。

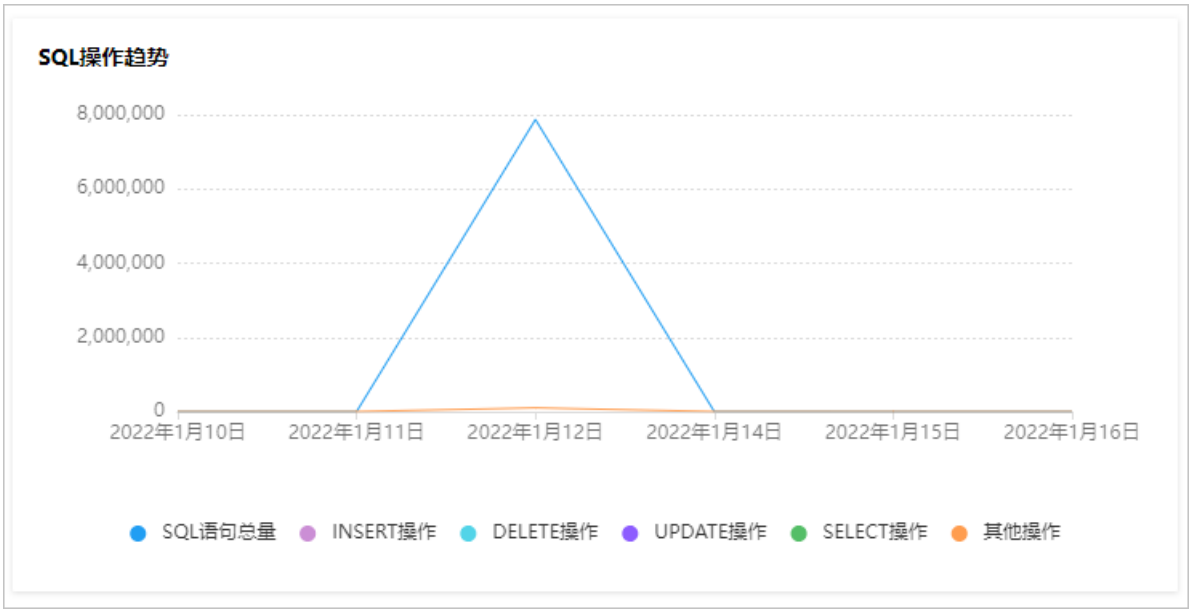
审计告警总览

审计告警总览展示您当前账号下检测出的审计风险和告警事件的统计数据图表，具体包含以下内容。

- **审计趋势**：展示所选时间范围内审计事件、泄漏风险事件、已处理泄漏风险事件的数量趋势。

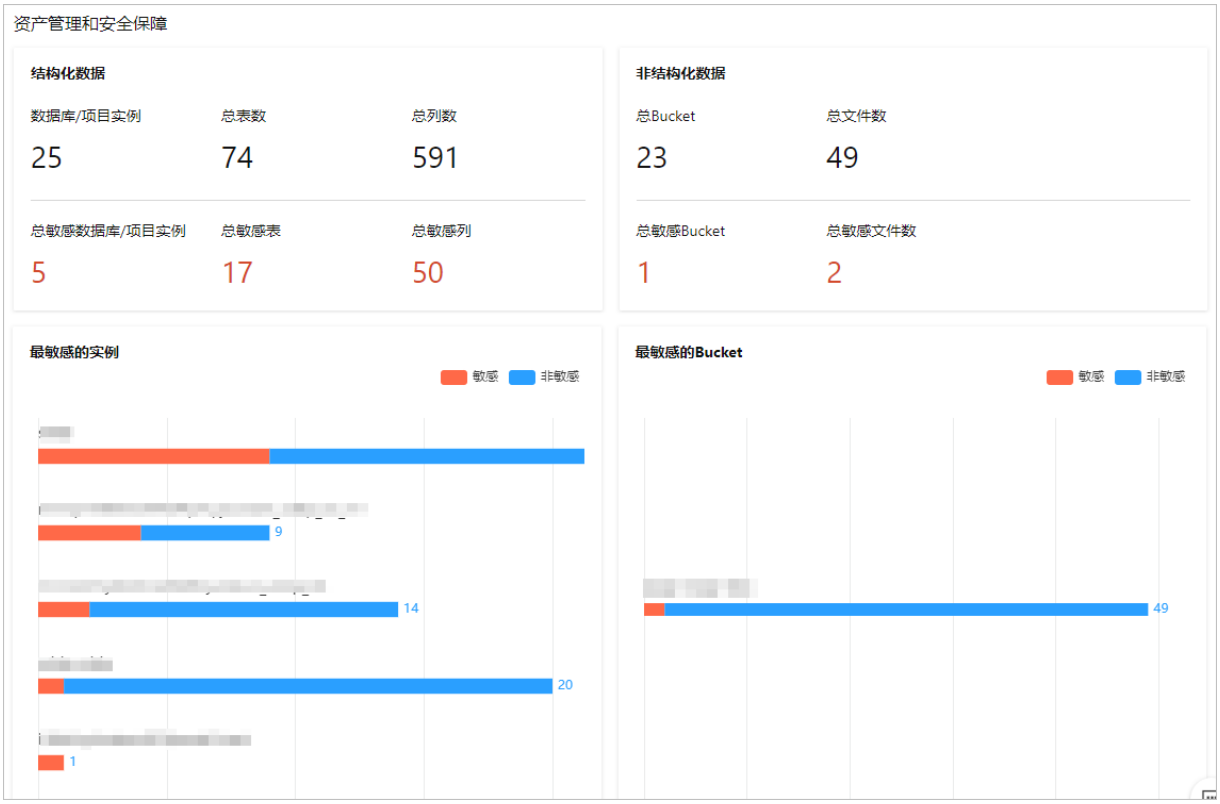


- **审计总数**：展示审计事件的统计数量。
- **告警总数**：展示告警事件的统计数量。
- **会话总数**：登录数据库的日志统计数量。
- **SQL操作趋势**：展示SQL语句数量和不同类型的操作数量。



- **最新告警**：展示最新告警事件的信息。

资产管理和安全保障



资产管理和安全保障：展示您当前账号下资产的总数及包含敏感数据的资产数量，具体包含以下内容。

- **结构化数据**：展示您数据库、项目实例的总量和敏感数据的数量，包括**数据库/项目实例**总数、**总表数**、**总列数**、**总敏感数据库/项目实例**、**总敏感表**和**总敏感列**。
- **非结构化数据**：展示您OSS数据的总量及敏感数据的数量，包括**总Bucket**、**总文件数**、**总敏感Bucket**数和**总敏感文件数**。
- **最敏感的实例**：展示您RDS、DRDS、OTS（表格存储）、ECS自建数据库和MaxCompute等数据源中存在

的敏感数据的实例或项目名称，及每个敏感实例中敏感表、非敏感表的数量。

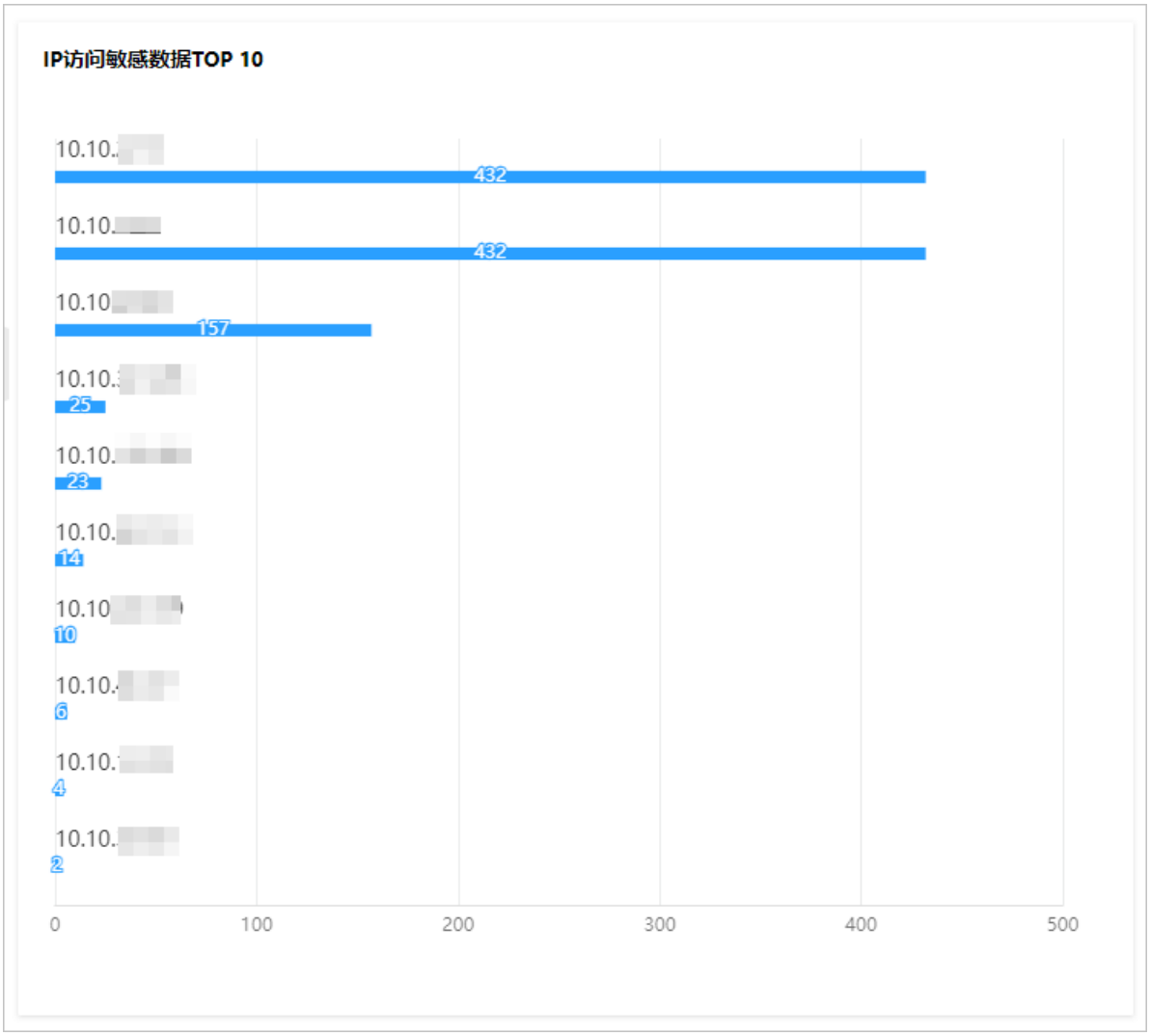
- **最敏感的Bucket**：展示您OSS数据中出现敏感数据的Bucket名称及每个敏感Bucket的敏感文件和非敏感文件数量。

审计告警和泄漏风险



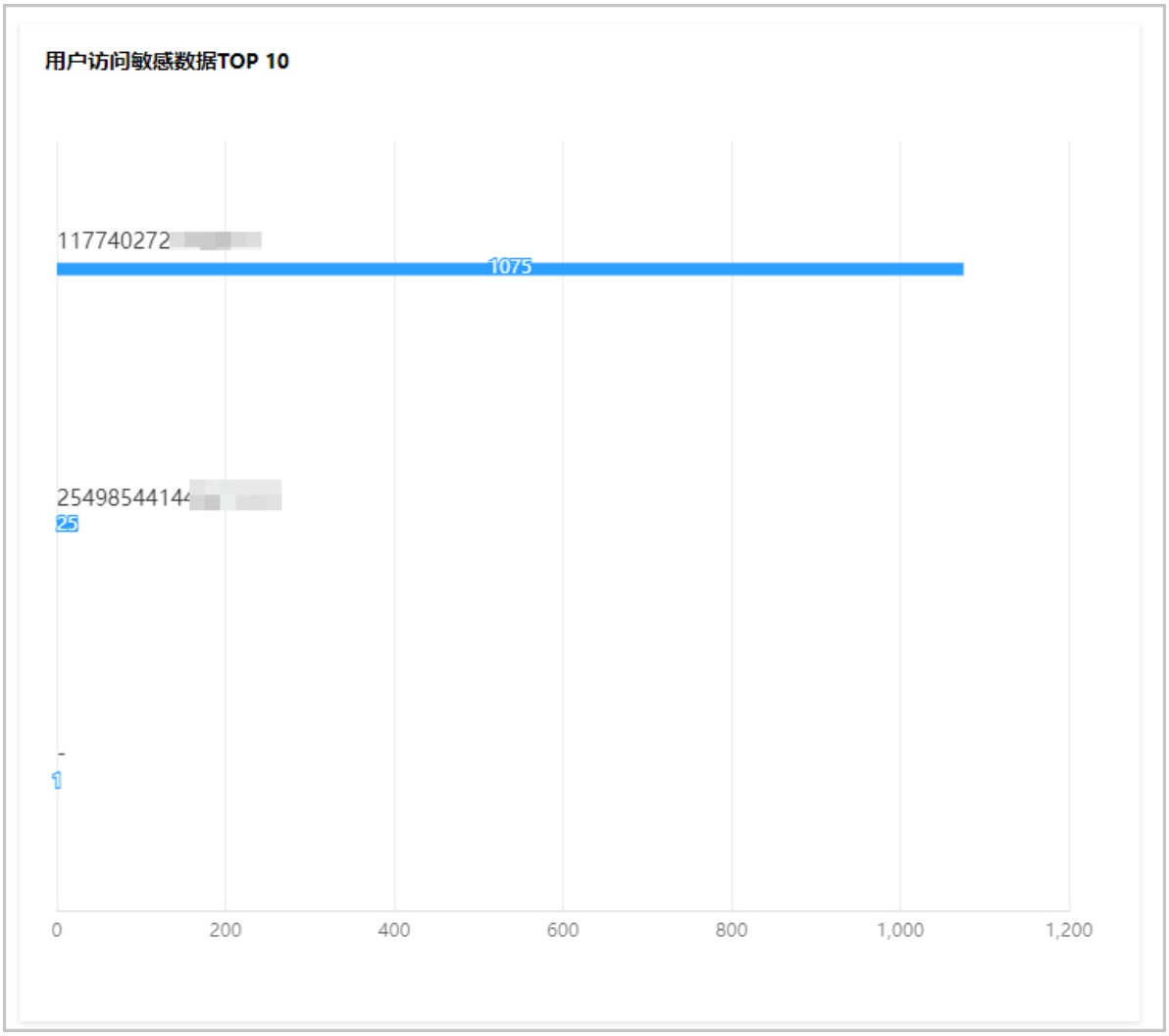
审计告警和泄漏风险展示您当前账号下检测出的异常事件和审计风险的统计数据图表，具体包含以下内容。

- **实例异常和审计事件分布**、**Bucket异常和审计事件分布**：展示您RDS、MaxCompute和OSS存储空间（Bucket）中异常事件和审计事件占统计数据的比例。
- **泄漏风险分类**：展示不同类型的泄漏风险事件在总泄漏风险事件中占比分布。
- **审计风险分布情况**：展示高、中、低类型的审计风险的分布情况。
- **IP访问敏感数据TOP 10**：展示访问敏感数据排名前10的IP地址及访问次数。



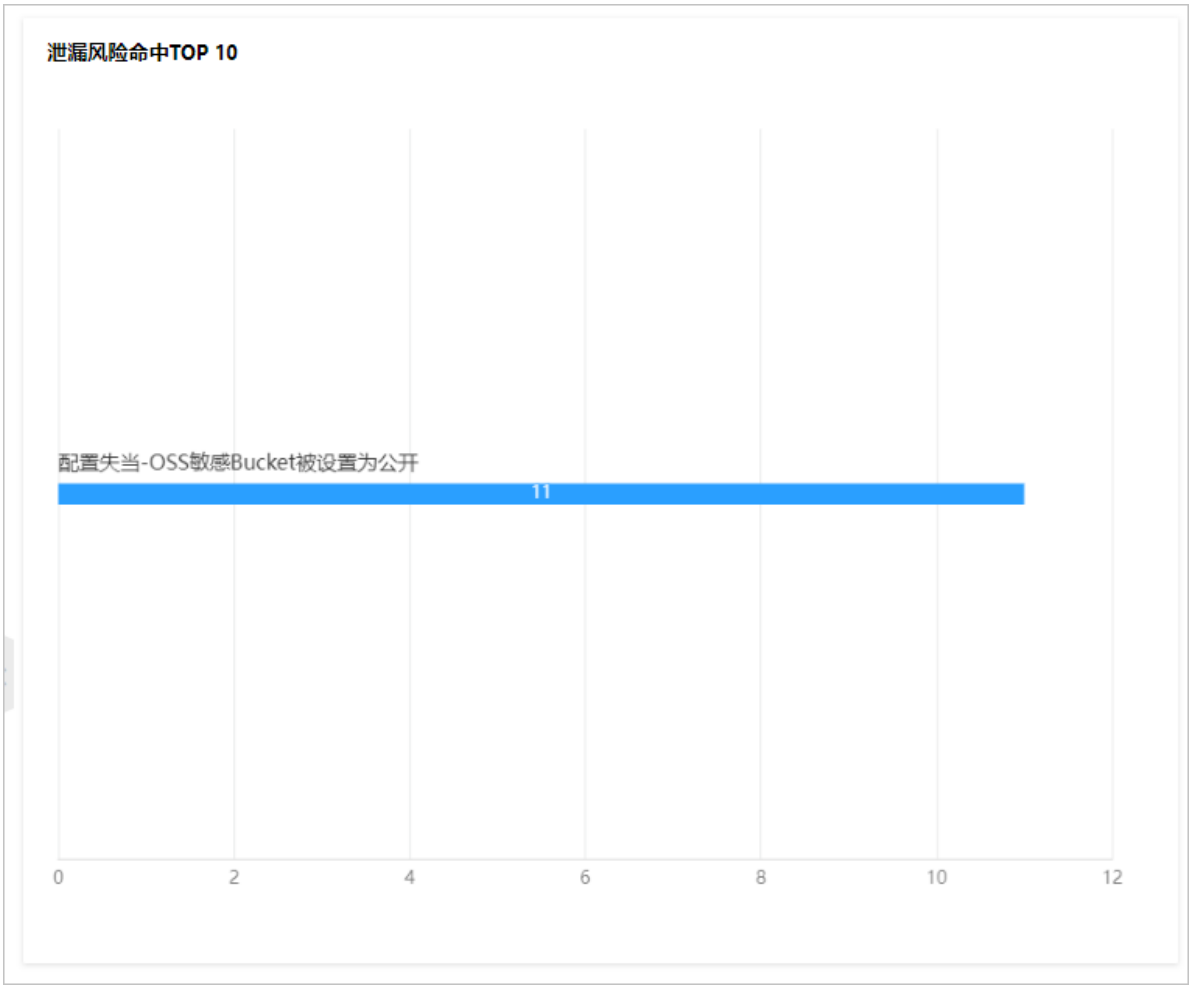
> **说明** 同一IP地址多次访问敏感数据，可能会造成敏感数据泄露，建议您重点关注及时排除数据泄露隐患。

- **用户访问敏感数据TOP 10**：展示访问敏感数据排名前10的用户名称及访问次数。



说明 同一用户多次访问敏感数据，可能会造成敏感数据泄露，建议您及时排查访问授权配置是否正确。

- **泄漏风险命中TOP 10**：展示检测出泄漏风险异常事件数量排名前10的泄漏风险异常事件事件子类型名称及命中次数。



- **审计命中规则TOP 10**：展示命中次数排名前10的审计规则名称及命中次数。审计规则的更多信息请参见审计规则。

安全性变化



安全性变化展示异常检测和审计规则检测出的新增异常事件的统计信息。具体包含以下内容。

- **安全异常**：展示异常检测出的新增异常事件、未处理异常、已处理异常、事件的风险类型的统计数据。
- **安全审计**：展示审计规则检测出的异常事件、用户异常事件、IP异常事件和事件风险类型的统计数据。

10.4.4.2. 原始日志

敏感数据保护（SDDP）的原始日志页面展示了资产的实例、库、账号、源IP地址、返回行数、时间等日志信息，您可通过搜索功能查看原始日志及其详细信息。

背景信息

SDDP支持获取已完成扫描授权资产对应的原始日志数据。

> **说明** 目前，SDDP支持查看OSS、RDS、OTS、DRDS、MaxCompute、MaxCompute-Audit、ADB-MYSQL、ADB-PG、ECS自建数据库、OceanDB产品的原始日志，暂不支持PolarDB。**MaxCompute**页签展示了MaxCompute产品的数据下载日志，**MaxCompute-Audit**页签展示了MaxCompute产品的SQL操作日志。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**数据安全审计 > 原始日志**。
4. 在**原始日志**页面，根据需要执行以下操作查看日志信息。

   > **说明** SDDP的**原始日志**页面默认显示最近1天的原始日志信息。

   - **根据搜索功能定位查看相关审计日志**：可根据以下筛选条件查看相关日志。
     - **时间**：在日志列表上方，单击时间搜索框右侧的 图标，依次选择开始日期和时间、结束日期和时间，并单击**确定**。



- **设置搜索条件**：在日志列表上方，输入实例、库、账号、项目等条件或选择操作类型，单击**搜索**。

  > 说明
  > - 不同的数据源支持的搜索条件不同，请您根据控制台实际显示的搜索条件进行搜索。
  > - 搜索条件支持模糊查询。
  > - 不同产品对应的操作类型说明请参见操作类型说明。

- **查看日志详情**：在日志列表中，定位到目标资产的数据项，单击其**操作**列的**详情**，查看日志详情，包括**客户端信息**、**服务端信息**和**行为信息**。

操作类型说明

OSS支持的操作类型

操作类型	说明
AbortMultiPartUpload	终止MultipartUpload事件。
AppendObject	以追加写的方式上传文件（Object）。
CompleteUploadPart	完成断点上传。
CopyObject	复制文件（Object）。
DeleteBucket	删除存储空间（Bucket）。
DeleteBucketEncryption	删除存储空间（Bucket）加密规则。
DeleteMultipleObjects	删除同一个存储空间（Bucket）中的多个文件（Object）。
DeleteObject	删除单个文件（Object）。
DeleteObjects	删除多个文件（Object）。
GetBucket	列举存储空间（Bucket）。
GetBucketAcl	获取存储空间（Bucket）权限。
GetBucketCors	查看存储空间（Bucket）的跨域资源共享（CORS）配置。
GetBucketEncryption	获取存储空间（Bucket）的加密规则。
GetBucketInfo	查看存储空间（Bucket）信息。
GetBucketLifecycle	查看存储空间（Bucket）的生命周期（Lifecycle）配置。
GetBucketLocation	查看存储空间（Bucket）地域。
GetBucketLog	查看存储空间（Bucket）访问日志配置。
GetBucketReferer	查看存储空间（Bucket）的防盗链（Referer）相关配置。

操作类型	说明
GetBucketReplication	查看跨地域复制。
GetBucketReplicationLocation	查看跨地域复制可同步的目标地域。
GetBucketReplicationProgress	查看跨地域复制进度。
GetBucketStat	获取存储空间（Bucket）的相关信息。
GetBucketWebSite	查看存储空间（Bucket）的静态网站托管状态。
get_image_info	获取图片的长宽等信息。
get_image_infoexif	获取图片的长宽以及exif信息。
GetObject	读取文件（Object）。
GetObjectAcl	获取文件（Object）访问权限。
GetObjectInfo	获取文件（Object）信息。
GetObjectMeta	查看文件（Object）元数据信息。
GetPartData	获取断点文件块数据。
GetPartInfo	获取断点文件块信息。
GetService	获取存储空间（Bucket）列表信息
HeadBucket	查看存储空间（Bucket）信息。
HeadObject	查看文件（Object）信息。
InitiateMultipartUpload	初始化断点上传文件。
ListCname	列举规范名称。
ListMultiPartUploads	列举断点事件。
ListParts	列举断点块状态。
list_style	列举存储空间（Bucket）的样式。
ListUserRegions	列举用户区域。
PostObject	使用HTML表单上传Object到指定存储空间（Bucket）。
ProcessImage	处理图片。
PutBucket	创建存储空间（Bucket）。
PutBucketAcl	设置或修改存储空间（Bucket）的访问权限（ACL）。

操作类型	说明
PutBucketEncryption	配置存储空间（Bucket）的加密规则。
PutObject	上传文件（Object）。
PutObjectAcl	修改文件访问权限。
PutObjectSymlink	创建Symlink文件。
RedirectBucket	Bucket Endpoint重定向。
UploadPart	断点上传文件。
UploadPartCopy	复制文件块。

RDS、DRDS、ADB-PG和OceanDB支持的操作类型

操作类型	说明
Alter	修改数据库。
Create	创建数据表。
CreateIndex	创建索引。
Delete	删除数据。
Drop	删除数据库。
DropIndex	删除索引。
Insert	插入数据。
Merge	合并数据。
Select	查看数据。
Update	修改数据。

OTS支持的操作类型

操作类型	说明
ComputeSplitPointsBySize	将全表的数据在逻辑上划分成接近指定大小的若干分片。
GetRange	读取指定主键范围内的数据。
GetRow	根据指定的主键读取单行数据。
ListTable	获取当前实例下已创建的所有表的表名。
PutRow	插入数据到指定的行。

MaxCompute和MaxCompute-Audit支持的操作类型

操作类型	说明
DOWNLOAD	下载操作。
UPLOAD	上传操作。
Alter	修改数据库。
Create	创建数据表。
Delete	删除数据。
Drop	删除数据库。
Insert	插入数据。
Select	查看数据。

10.4.4.3. 会话信息

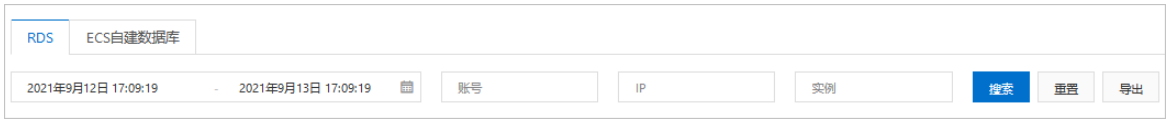
敏感数据保护会话信息页面展示登录您RDS、ECS自建数据库的会话信息。本文介绍如何查看登录RDS、ECS自建数据库的会话。

背景信息

如果您发现RDS、ECS自建数据库被异常登录或修改，您可以在**数据安全审计 > 会话信息**页面查看数据库登录会话的详细记录。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据安全审计 > 会话信息**。
4. 在**RDS**或**ECS自建数据库**页签设置搜索条件并单击**搜索**。



支持设置以下搜索条件：

- **时间**：设置需要搜索的会话的开始时间和结束时间。
- **账号**：输入登录数据库的账号名称。支持模糊搜索。
- **IP**：输入登录会话使用的IP地址。请输入完整IP地址，不支持模糊搜索。
- **实例**：输入实例名称。支持模糊搜索。
- **数据库**：在**ECS自建数据库**页面，支持通过数据库名称搜索。

5. 定位到目标会话，单击操作列下的**详情**。
6. 在**详情**面板，查看当前会话的详细信息。

您可以查看登录源的客户端IP地址、登录时间、登出时间、会话时长等详细信息。

10.4.4.4. 异常告警

敏感数据保护SDDP的异常告警页面展示了资产命中审计规则结果、命中规则的操作类型和操作账号等事件信息，您可通过搜索功能查看告警事件及其详细信息。

背景信息

SDDP可根据系统内置的默认审计规则或自定义的审计规则抓取对应的异常告警事件数据。 更多信息请参见审计规则。

> **说明** 目前，SDDP支持查看OSS、RDS、OTS、MaxCompute、DRDS、ADB-PG、ADB-MYSQL、ECS自建数据库、DataWorks、OceanDB数据的异常告警事件，暂不支持PolarDB。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**数据安全审计 > 异常告警**。
4. 在**异常告警**页面，根据您需要查看的数据类型单击数据源页签，包含**OSS**、**RDS**、**OTS**、**MaxCompute**、**DRDS**、**ADB-PG**、**ADB-MYSQL**、**ECS自建数据库**、**DataWorks**或**OceanDB**页签。
5. 在**OSS**、**RDS**、**OTS**、**MaxCompute**、**DRDS**、**ADB-PG**、**ADB-MYSQL**、**ECS自建数据库**、**DataWorks**或**OceanDB**页签中，根据需要执行以下操作查看异常告警信息。

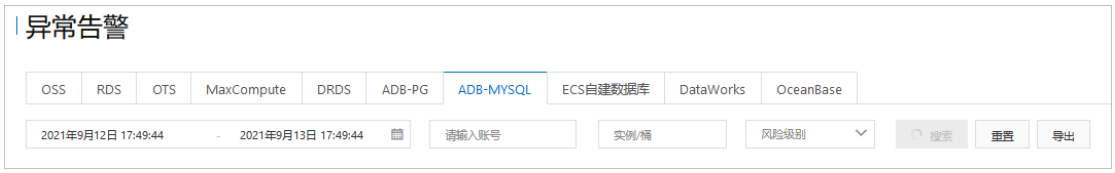
   > **说明** 异常告警页面默认展示最近1天的异常告警信息。

   - **根据搜索功能定位查看相关异常告警**：可根据以下筛选条件查看相关异常告警。
     - **时间**：在告警事件列表上方，单击时间搜索框右侧的 图标，依次选择开始日期和时间、结束日期和时间，并单击**确定**。



- **搜索事件**：在事件列表上方，输入**账号**、**实例/桶**或选择**风险级别**（高、中、低），单击**搜索**。

  > **说明** 账号和实例/桶支持模糊搜索。

  您可以在异常告警列表中查看满足搜索条件的异常告警信息，异常告警列表支持**分析模式**、**列表模式**，各数据类型支持的模式如下所示：

  - 在**RDS**、**DRDS**、**ECS自建数据库**、**DataWorks**或**OceanDB**页签，支持**分析模式**、**列表模式**。
  - 在**OSS**、**OTS**、**MaxCompute**、**ADB-PG**、**ADB-MYSQL**页签，支持**列表模式**。

- **查看事件详情**：在事件列表中，定位到目标事件项，单击其**操作**栏的**详情**，可以查看异常告警详情和原始日志信息。
  - **告警**

    在**告警**页签可以查看风险级别和命中规则信息。
  - **原始日志**

    单击**原始日志**页签，可以查看客户端信息、服务端信息和行为信息的详情。

10.4.4.5. 审计规则

10.4.4.5.1. 创建自定义规则

本文介绍了如何创建敏感数据保护自定义审计规则，SDDP会根据您自定义的审计规则抓取对应的审计日志数据。

背景信息

SDDP支持审计日志功能，审计日志数据提供了包括审计规则命中结果、审计规则检测的资产类型、命中规则的操作类型和操作账号等信息，覆盖资产数据产生、更新和使用等全链路的日志数据。

> **说明** SDDP支持审计OSS、RDS、OTS（即表格存储）、MaxCompute、DRDS、ADS、GPDB、OceanDB、PolarDB数据。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在**敏感数据保护**界面左侧导航栏中，选择**云原生数据审计 > 审计规则**。
4. 在**审计规则**页面，单击**自定义规则**页签。
5. 在**自定义规则**页签，单击**新增规则**。
6. 在**新增规则**页面，配置审计规则相应参数。



您可以参考以下表格中的参数说明配置防护策略。

参数	说明
规则名称	自定义审计规则的名称，建议输入有实际意义的名称以便有效识别该审计规则。
规则类型	从下拉列表选择该审计规则的规则类型，支持选择以下类型： ○ **高危操作** ○ **SQL注入** ○ **漏洞攻击**
风险级别	从下拉列表选择该审计规则的风险等级，支持选择以下风险级别： ○ **高** ○ **中** ○ **低**

参数	说明
资产类型	请选择审计规则生效的资产类型。支持选择以下资产类型： ○ OSS ○ RDS ○ DRDS ○ OTS ○ MaxCompute ○ PolarDB ○ ADB-PG ○ ADB-MYSQL ○ OceanBase
行为信息	输入审计规则的说明信息。
规则描述	根据实际需要配置规则条件，SDDP将在规则条件限定的范围内采集审计数据。
添加	单击**添加**，完成当前规则的配置。支持添加多条规则。

7. 单击**提交**。

   审计规则创建完成后，您可以在**审计规则**列表中查看该审计规则的开启状态、命中次数和详情信息，或修改该审计规则。

   > **说明** 创建完成后，审计规则的**状态**默认为*开启*。您也可在**审计规则**列表中手动开启或关闭审计规则。
   >
   > 关闭该审计规则后，SDDP不会再执行该审计规则项抓取审计日志数据。

后续步骤

创建并开启审计规则后，SDDP将在5分钟内同步审计结果，您可在**异常告警**页面查看相关告警数据。更多信息，请参见异常告警。

10.4.4.5.2. 查看内置规则

本文介绍了如何查看内置规则。

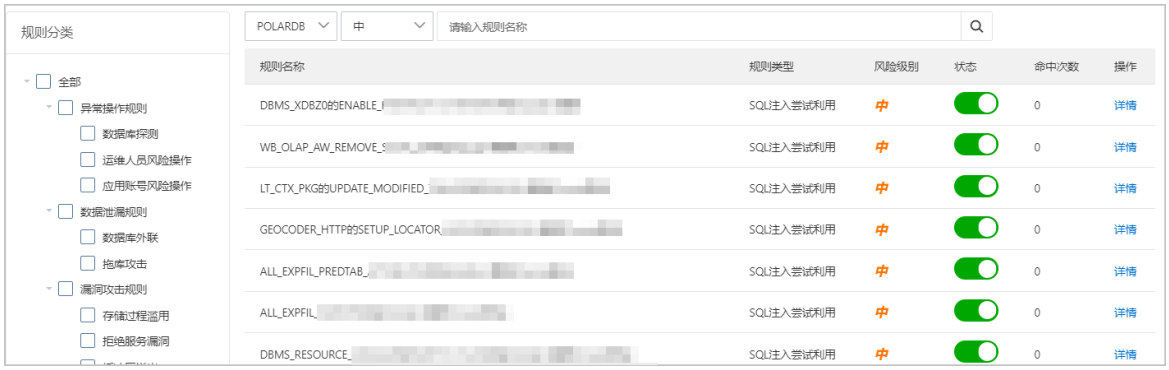
1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在**敏感数据保护**界面左侧导航栏中，选择**云原生数据审计 > 审计规则**。
4. 在**审计规则**页面，单击**内置规则**页签。
5. 在**内置规则**页签，单击**数据库审计规则**、**OSS审计规则**或**MaxCompute审计规则**。
6. 设置搜索条件，单击搜索图标。



搜索条件	说明
资产类型	请选择审计规则生效的资产类型。支持选择以下资产类型： ○ RDS ○ DRDS ○ POLARDB ○ OTS ○ OB ○ ADS ○ MongoDB ○ Redis ○ Dataphin 仅**数据库审计规则**支持按**资产类型**搜索，**OSS审计规则**和**MaxCompute审计规则**不支持。
风险级别	从下拉列表选择该审计规则的风险等级，支持选择以下风险级别： ○ **高** ○ **中** ○ **低**
规则名称	输入内置审计规则的名称。

7. 在审计规则列表中，查看审计规则的**规则名称**、**规则类型**、**风险级别**、**状态**、**命中次数**等信息。

   您还可以通过审计规则列表左侧的**规则分类**栏目对审计规则进行筛选。



   - 修改规则状态：通过开启或关闭指定规则**状态**列的开关，开启或关闭规则。
   - 查看规则详情：单击指定规则**操作**列的**详情**，您可以查看该规则的基本信息。

10.4.5. 数据权限

10.4.5.1. 查看权限统计

本文介绍如何查看权限统计结果。

背景信息

通过权限管理，了解专有云的整体权限分布结果。通过该功能，管理员能够快速分辨出高风险的账号和人员，及时进行安全排查和整改。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**页面。
3. 在左侧导航栏，选择**数据权限 > 权限管理**页面。
4. 查看整体的权限统计情况。



   - **可访问敏感数据的账号数**：能够访问敏感数的账号数量。
   - **部门总数**：专有云的所有部门数量。
   - **人员总数**：专有云的所有使用人员数量。
   - **账号总数**：专有云的所有账号数量。
5. 查看部门级权限情况统计。

   以部门为维度，查看使用人员数量、各类型账号数量、各类型异常事件数量和权限异常数量。

10.4.5.2. 检索权限

本文介绍如何检索权限。

背景信息

通过检索账号，查看该账号的人员信息，管理员可以快速定位敏感数据的责任人。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**数据安全**区域单击**敏感数据保护**。
3. 在左侧导航栏，选择**数据权限 > 权限检索**。



4. 检索需要查看的具体账号。

   通过搜索方式查找账号，步骤如下。

   i. 在下拉菜单中，选中**部门**（或者**员工**）。

   ii. 在输入框中，输入部门、账号等关键字。

   iii. 单击**查询**，在**显示名**中查看搜索结果。

   > **说明** 您也可以在部门名称下选择具体部门，在显示名中可以查看该部门所有账号。

5. 在**显示名**中，单击需要查看的账号。
6. 在右侧查看该账号的**个人信息**和**账号信息**。
   - **个人信息**

     查看个人的联系方式，违例确认权限异常事件数和违例排除权限异常事件数。
   - **账号信息**

     查看可操作云账号、账号类型、账号创建时间、可操作产品等信息。

     通过**查看账号权限**，查看账号下的资源、资源类型、资源路径、操作权限等信息。

10.4.6. 数据流转监控

10.4.6.1. 查看DataHub

本文介绍如何查看DataHub。

背景信息

DataHub是流式数据（Streaming Data）的处理平台，提供对流式数据的发布（Publish）、订阅（Subscribe）及分发功能，让您可以轻松构建基于流式数据的分析和应用。

在**DataHub**中，支持Datahub的数据流转详情展示，层次化展示Datahub中项目与Topic的对应关系，层次化展示Topic与订阅、归档的对应关系。

操作步骤

1.
2. 在控制台上方选择**安全 > 数据安全 > 敏感数据保护**。
3. 在敏感数据保护页面左侧导航栏，选择**数据流转监控 > DataHub**。
4. 在搜索区域，输入部门关键字并选择部门，在**DataHub主题搜索**中输入主题关键字，单击**查询**。



> **说明**
>
> 您也可以在下方区域，直接通过选择**项目名称**和**主题名称**，快速定位到DataHub主题。

在DataHub主题中，可以查看该主题的**项目信息**和**topic信息**。

- **项目信息**

  包含项目名、云账号、创建人、创建时间、主题数等信息。

- **topic信息**

  包含名称、云账号、创建人、创建时间、类型等信息。

5. 单击**查看订阅**，查看订阅列表。

   订阅列表包含订阅名、创建人云账号、显示名、订阅应用名称、应用接口人等信息。



i. 在搜索区域，输入部门关键字并选择部门。

ii. 在**订阅名**中输入订阅名关键字。

iii. 单击**查询**，可以快速定位到订阅名主题。

6. 单击**查看归档**，查看归档列表。

   归档列表中包含连接实例名、创建人云账号、显示名、归档产品源、资源路径、风险等级等信息。

   i. 在搜索区域，输入部门关键字并选择部门。

   ii. 在**连接实例名**中输入实例名关键字。

   iii. 单击**查询**，可以快速定位到对应实例。

10.4.7. 数据脱敏

10.4.7.1. 新增静态脱敏任务

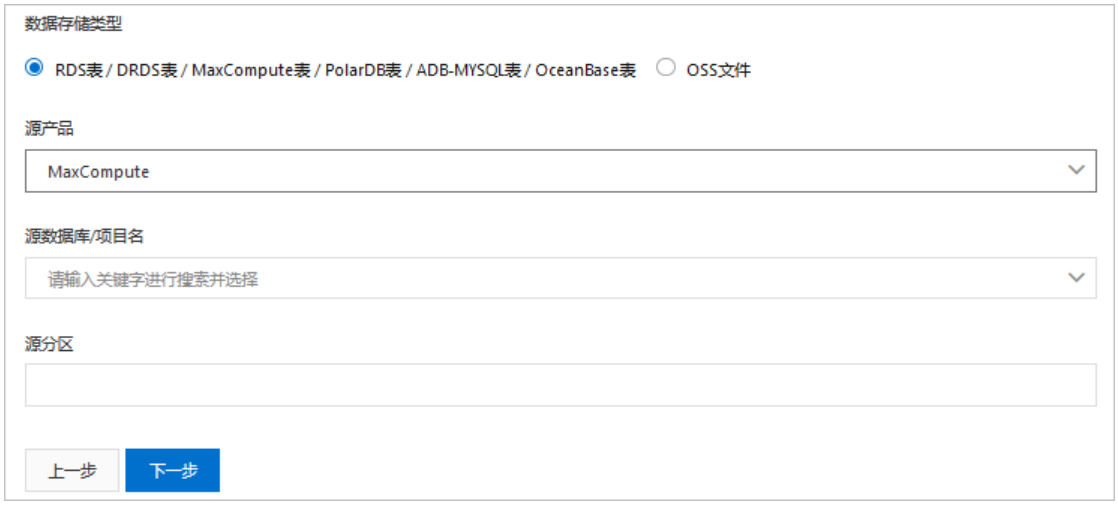
本文介绍如何新增静态脱敏任务，并执行任务对敏感数据进行脱敏。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**数据脱敏 > 静态脱敏**。
4. 在**脱敏任务配置**页签，单击右上角的**新增脱敏任务**。
5. 在**新增脱敏任务**页面，配置任务参数。

   i. 在**任务基本信息**中，配置**任务名称**和创建**任务备注**，单击**下一步**。

   ii. 在**脱敏源配置**中，设置脱敏源，单击**下一步**。



敏感数据保护支持对RDS表、MaxCompute表、OceanBase表或OSS文件等数据源新增脱敏任务。配置脱敏源时，参数说明如下表所示。

数据源	参数	说明
MaxCompute	**数据存储类型**	选择**RDS表 / DRDS表 / MaxCompute表 / PolarDB表 / ADB-MYSQL表 / OceanBase表**。
	源产品	选择**MaxCompute**。
	源数据库/项目名	在下拉列表中，选择包含脱敏数据的表所在的源数据库或项目名称。
	源表名	在下拉列表中，选择脱敏数据所在的数据表名称。
	源分区	手动输入需要脱敏的数据在数据表中的分区名称。 分区是指在创建MaxCompute数据表时指定的分区空间，用于限定不同区域，方便快速和高效地对指定内容进行查询。 **说明** **源分区**为选填项，不填写则代表会对整个表中的敏感数据进行脱敏。
RDS、DRDS、OceanBase	**数据存储类型**	选择**RDS表 / DRDS表 / MaxCompute表 / PolarDB表 / ADB-MYSQL表 / OceanBase表**。
	源产品	选择**RDS、DRDS或OceanBase**。
	源数据库/项目名	在下拉列表中，选择包含脱敏数据的表所在的源数据库或项目名称。
	源表名	在下拉列表中，选择脱敏数据所在的数据表名称。
	抽样SQL	选填项。手动输入SQL语句可选择脱敏数据范围。
	源类型选择	选择**RDS表 / DRDS表 / MaxCompute表 / PolarDB表 / ADB-MYSQL表 / OceanBase表**。

数据源	参数	说明
ADB-MYSQL表、PolarDB表	**源产品**	选择**ADS**或**PolarDB**。
	源数据库/项目名	在下拉列表中，选择包含脱敏数据的表所在的项目名称。
	源表名	在下拉列表中，选择脱敏数据所在的数据表名称。
自建数据库	**源类型选择**	选择**OSS文件**。
	文件源	支持**本地上传**或选择**OSS Bucket**。可选值： ■ **本地上传**：单击**选择本地文件**，选择本地源文件。 ■ **OSS Bucket**：选择Bucket源文件。
	源文件描述	输入Bucket的备注内容，便于您后续查看时能快速识别。 **说明** 仅**文件源**设置为**本地上传**时，需要设置。
	源文件选择	选择OSS的Bucket源文件。 **说明** 仅**文件源**设置为**OSS Bucket**时，需要设置。
	源文件名称	选填项。手动输入Bucket的名称。 **说明** 仅**文件源**设置为**OSS Bucket**时，需要设置。 如需开启通配符，打开**开启通配**开关。开启通配后，您可以使用*方式指定一批源文件进行批量脱敏，目前仅支持对文件名前缀进行匹配，例如test*.xls。设置批量脱敏后，系统会采用相同的规则进行脱敏，请务必保证这批文件有相同的列结构。
	分隔符选择	选填项。对于CSV和TXT类型的文件，需要指定列分隔符，请根据源文件类型进行选择。支持选择以下类型分隔符： ■ **分号“;”（MacOS、Linux默认）** ■ **逗号“,”（Windows默认）**
	表格包含标题行	选填项。根据需要选择待脱敏表格是否包含标题行。

iii. 在**脱敏算法**中，配置脱敏算法，单击**下一步**。

在脱敏算法配置表格中，对需要进行脱敏的源字段配置算法种类、选择算法并开启脱敏开关。

iv. （可选）在**数据水印**中，开启**开启数据水印**开关。选择嵌入水印的字段、水印算法，输入水印信息，单击**下一步**。

水印算法支持如下两种算法：

- **空格算法**：适用于嵌入字段类型为字符型的场景。
- **修改最低有效位算法**：适用于嵌入字段类型为数值型的场景。

v. 在**目标位置配置**中，设置敏感文件的**目标数据库/项目名**、**输入目标表名**等目标位置信息，测试写入权限，单击**下一步**。

vi. 在**处理逻辑确认**中，确认处理逻辑。

参数	说明
触发方式选择	触发方式表示执行脱敏任务的方式。可选项： - **仅人工**：需要在静态脱敏配置页面，通过手动的方式启动脱敏任务。 - **仅定时触发**：通过设置的时间点定时自动执行脱敏任务，可选每小时、每天、每月固定时间点自动触发任务。 - **人工+定时触发**：默认在设置的时间点自动执行脱敏任务，可选每小时、每天、每月固定时间点；同时支持手动方式启动脱敏任务。
开启增量脱敏	选填项。您可根据需要选择是否开启增量脱敏。增量脱敏是指每次脱敏数据为上次脱敏任务完成后新增的数据的脱敏方式。您需要选择一个源数据中随着时间递增的字段作为增量列，例如创建时间、自增ID（数据库自带的自增列）等。 **说明** 当前仅支持RDS的增量脱敏。
分片字段	选填项。SDDP执行静态脱敏时会对源数据进行字段分片，通过并发处理的方式提高脱敏效率。您可根据需要选择分片字段，支持选择多个分片字段。 **说明** - 当前仅有RDS数据支持增量脱敏，建议使用主键或者唯一索引作为分片字段。 - 分片字段选择框内如果未选取任何字段，SDDP将会默认使用主键作为分片字段，对源数据进行脱敏处理。如果您的源数据中没有主键，您必须选择分片字段，否则会导致脱敏任务失败。 - 过多的分片字段会影响查询性能以及数据准确性，请谨慎选择。
表名冲突解决	表名称存在冲突的情况下处理的方式。可选项： - **删除目标表建同名新表** - **在目标表附加数据**：建议选择该选项。
行冲突解决	行存在冲突的情况下处理的方式。可选项： - **保留目标表冲突行，丢弃新插入数据**：建议选择该选项。 - **删除目标表冲突行，新插入新增数据**

vii. 单击**提交**，完成脱敏任务的创建。

创建脱敏任务后，在**脱敏任务列表**中可以查询到该任务。

6. 在脱敏任务列表中，单击开启按钮，执行脱敏任务。
7. 在**任务执行状态**中，查看脱敏任务的**执行进度**和**状态**。

10.4.7.2. 查看动态脱敏API调用信息

SDDP提供了动态脱敏功能，您可以通过调用ExecDatamask接口对数据进行动态脱敏。

背景信息

调用该接口时需要传入脱敏模板ID。动态脱敏和静态脱敏可以共用已创建的脱敏模板。您可以在云盾控制台的**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 脱敏模板**页面，获取脱敏模板ID。您也可以新建脱敏模板，更多信息，请参见新增脱敏模板。



限制条件

您调用ExecDatamask接口对指定数据进行动态脱敏时，请求参数 `Data` 的数据大小必须小于2 MB。

调用动态脱敏接口记录说明

在云盾控制台**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 动态脱敏**页面，您可以查看调用ExecDatamask接口的详细操作记录，包括调用的接口名称、UID（阿里云账号或RAM用户的标识）、IP地址（发起调用的IP地址）、首次调用时间、最后一次调用时间和累计调用次数。



> **说明** 来自同一账号并且来源IP相同的调用只生成一条记录。同一账号和来源IP发生多次调用时会累计调用次数。

10.4.7.3. 新增脱敏模板

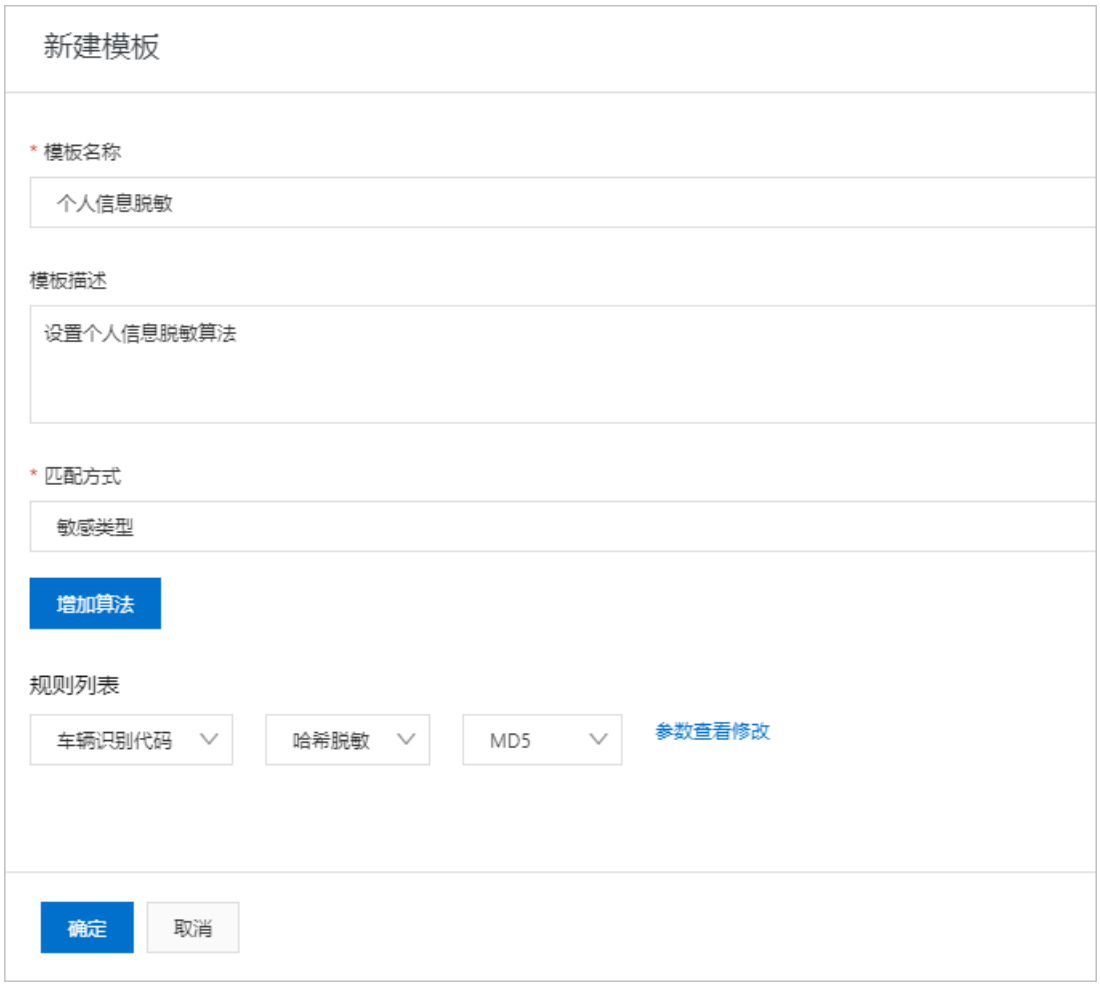
SDDP支持创建脱敏模板。您可以将使用频率较高且应用场景相同的脱敏算法配置在同一个脱敏模板中，避免重复地配置脱敏算法，提高处理敏感数据的效率。本文介绍如何新增和管理脱敏模板。

新增脱敏模板

您可以创建的脱敏模板数量没有限制。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。

3. 在左侧导航栏，选择**敏感数据脱敏 > 脱敏模板**。
4. 在**脱敏模板**页面，单击**新建模板**。
5. 在**新建模板**面板，参考以下表格配置模板参数。



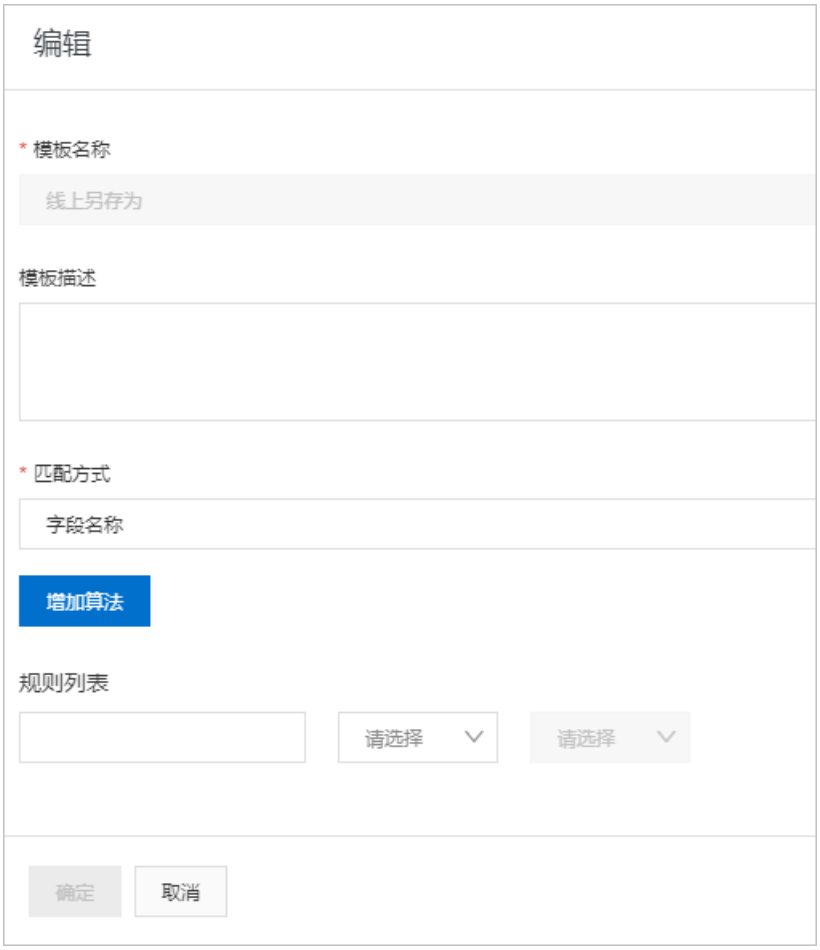
参数	说明
模板名称	脱敏模板的名称。
模板描述	脱敏模板的相关信息。您可以在此输入脱敏模板的使用范围等关键信息。
匹配方式	选择一种敏感数据的匹配方式，可以选择以下方式： ○ **敏感类型**：选择SDDP支持的敏感数据类型并设置相应的脱敏算法，例如车辆识别代码、统一社会信用代码等。 ○ **字段名称**：指定需要脱敏的字段名称并设置相应的脱敏算法。

参数	说明
规则列表	在规则列表中选择敏感类型或输入需要进行脱敏的字段，设置您需要使用的脱敏算法。SDDP支持以下脱敏算法： ○ 哈希脱敏 ○ 遮盖脱敏 ○ 替换脱敏 ○ 变换脱敏 ○ 加密脱敏 ○ 洗牌脱敏 ○ 数据解密 更多信息请参见配置脱敏算法。 您可以在一个模板中添加多个规则，单击**增加算法**可新增一条脱敏算法规则。

管理模板

- **编辑模板**

  如果需要更新指定脱敏模板的描述或规则，您可以在**脱敏模板**页面定位到该模板并单击其操作列的**编辑**，在**编辑**页面修改模板的描述或相关规则。



- **删除模板**

  如果某个模板不再适用于当前的业务场景，您可以在**脱敏模板**页面定位到该模板并单击其操作列的**删除**，删除该模板。

  > **说明** 模板删除后无法恢复，请谨慎操作。

10.4.7.4. 配置脱敏算法

本文介绍如何配置脱敏算法。

背景信息

SDDP支持的脱敏算法如下：

算法分类	分类描述	算法描述	输入参数	适用类型和典型场景
哈希脱敏	不可逆算法。 适用于需要通过密码或对比进行敏感数据确认的场景。 支持常见的哈希算法，并支持偏移量（加盐值）配置。	MD5	Salt值	• 敏感类型：密钥类 • 适用场景：数据存储
		SHA-1	Salt值	
		SHA-256	Salt值	
		HMAC	Salt值	
遮盖脱敏（*和#）	不可逆算法。 适用于前端展示或敏感数据分享的场景。 通过使用特殊字符（*或者#），对部分文字进行遮盖实现敏感数据的脱敏。	保留前n后m	n、m	• 敏感类型：个人敏感 • 适用场景： ○ 数据使用 ○ 数据分享
		保留自x至y	x、y	
		遮盖前n后m	n、m	
		遮盖自x至y	x、y	
		特殊字符前遮盖（针对首次出现该字符）	“@”、”&”、“.”	
		特殊字符后遮盖（针对首次出现该字符）	“@”、”&”、“.”	
替换脱敏	部分可逆算法。 适用于证件号等构成规则固定的字段脱敏。	身份证映射替换	行政区划随机码表	• 敏感类型： ○ 个人敏感 ○ 企业敏感
		身份证随机替换	行政区划随机码表	
		军官证随机替换	种类编码随机码表	
		护照随机替换	用途字段随机码	
		港澳通行证随机替换	用途字段随机码	
		银行卡随机替换	Bin码随机码表	
		座机号码随机替换	行政区划随机码表	

分类（支持新增分类）	分类描述	算法描述	输入参数	适用类型和典型场景
	使用替换码表进行映射替换（可逆），或使用随机区间进行随机替换（不可逆），实现字段整体或者部分内容的脱敏。系统预置多套码表可供选择，并支持用户自定义替换算法。	手机号随机替换	网号	○ 设备敏感 • 适用场景： ○ 数据存储 ○ 数据分享
		统一信用码随机替换	登记部门随机码表、类别码随机码表、行政区划随机码表	
		通用表格映射替换	大写字母映射码 、小写字母映射码、数字映射码、特殊映射码	
		通用表格随机替换	大写字母随机码 、小写字母随机码、数字随机码 、特殊随机码	
变换脱敏	部分可逆算法。 适用于对敏感数据集进行分析和统计类场景。 提供对数字或日期等进行取整操作（不可逆）和对文字进行位移操作（可逆）两类变换脱敏算法。	数字取整，保留小数点前第N位	N	• 敏感类型：通用敏感 • 适用场景： ○ 数据存储 ○ 数据使用
		日期取整	日期取整保留到	
		字符位移	整体循环位移Bit数、向左/向右	
加密脱敏	可逆算法。 适用于对需要回源的字段进行加密的场景。 支持常见的对称加密算法。	DES算法	加密密钥	• 敏感类型： ○ 个人敏感 ○ 企业敏感 • 适用场景：数据存储
		3DES算法	加密密钥	
		AES算法	加密密钥	
洗牌脱敏	不可逆算法。 适用于结构化数据列级别的数据脱敏场景。 在源数据表抽取数据并确认数值范围后，对该字段（在范围内）进行列级别的打散重排和随机选择，实现混淆脱敏。	随机洗牌	打散重排或随机选择	• 敏感类型： ○ 设备敏感 ○ 位置敏感 • 适用场景：数据存储

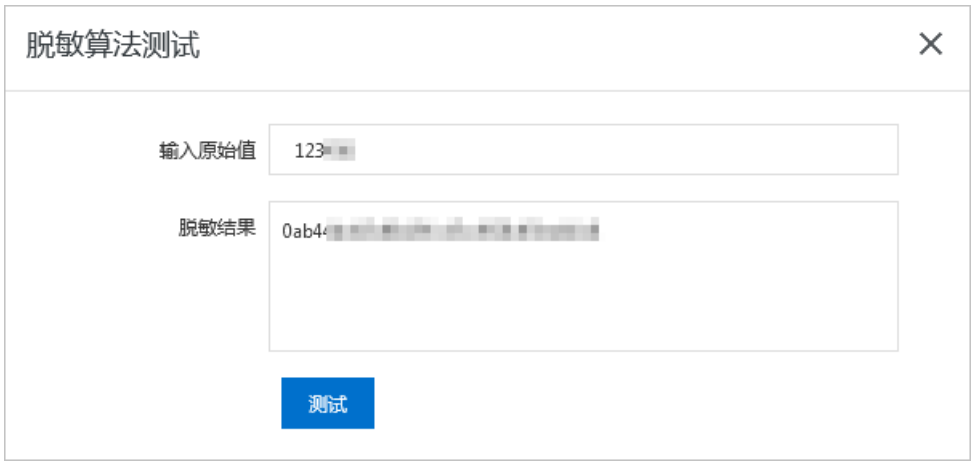
哈希脱敏

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**数据脱敏 > 脱敏算法**，在**脱敏算法**页面单击**哈希脱敏**页签。
4. 在各算法中设置盐值。

> **说明** 在密码学中，通过在密码任意固定位置插入特定的字符串，让散列后的结果和使用原始密码的散列结果不相符，这种过程称之为“加盐“。
>
> 盐值即插入的特定字符串。



5. 在**脱敏算法测试**面板，单击**测试**，测试是否脱敏。



6. 测试完成后，单击**提交**。

遮盖脱敏

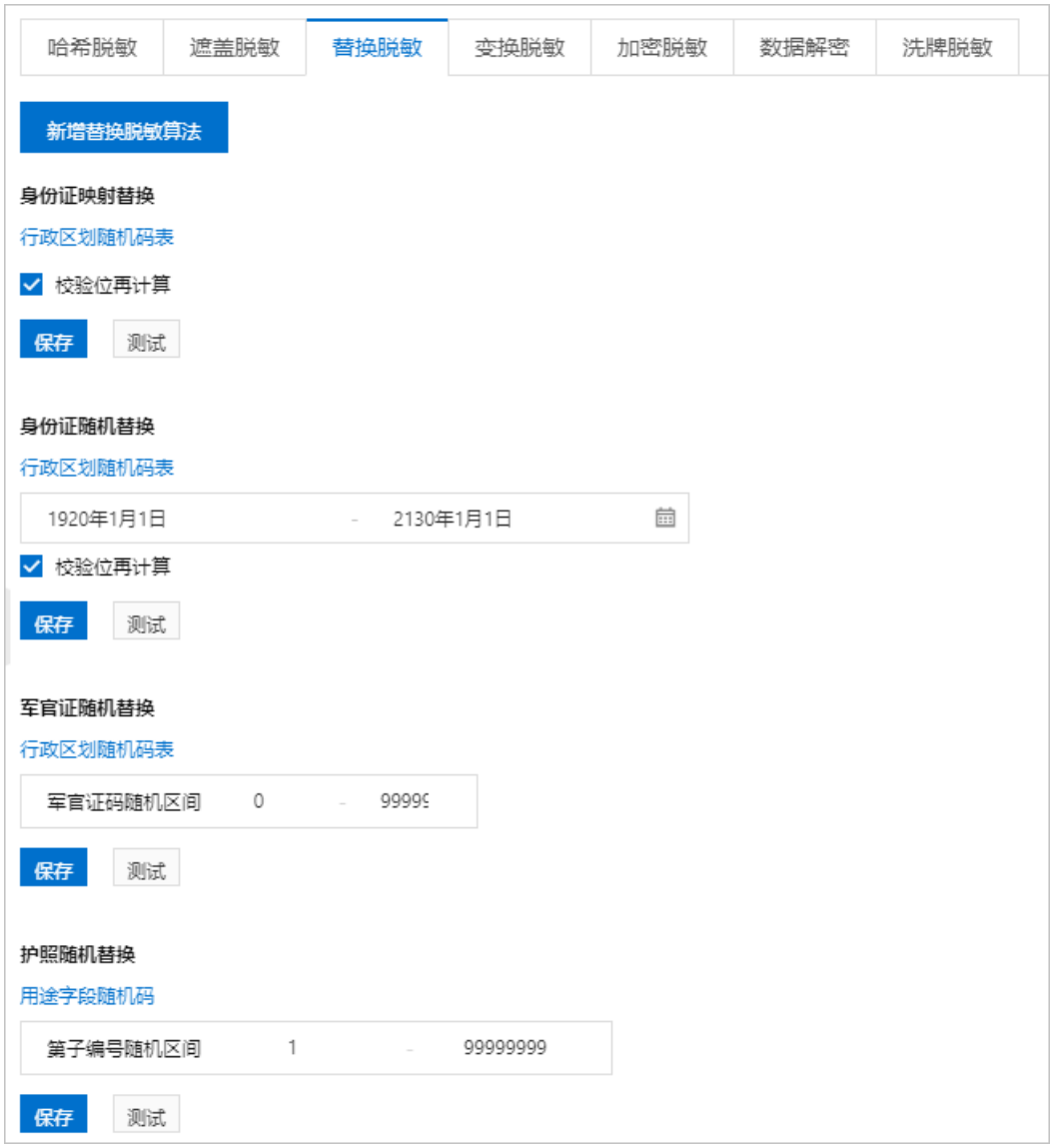
1. 登录云盾安全中心。
2. 在左侧导航栏，选择**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 脱敏算法**。
3. 在左侧导航栏，选择**数据脱敏 > 脱敏算法**，在**脱敏算法**页面单击**遮盖脱敏**页签。
4. 设置遮盖脱敏算法的参数。



5. 在**脱敏算法测试**面板，单击**测试**，测试是否脱敏。
6. 测试完成后，单击**提交**。

替换脱敏

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 脱敏算法**。
3. 在左侧导航栏，选择**数据脱敏 > 脱敏算法**，在**脱敏算法**页面单击**替换脱敏**页签。
4. 设置替换脱敏算法的参数。



> **说明** 系统已经默认提供常用的多个替换算法（例如身份证、手机号等）。

- 如果您需要自定义码表，单击对应码表，以自己的码表覆盖原有内容，并单击**保存**。
- 如果您需要自定义新的替换脱敏算法，单击**新增替换脱敏算法**，自定义脱敏区间和替换码表。

5. 在**脱敏算法测试**面板，单击**测试**，测试是否脱敏。
6. 测试完成后，单击**保存**。

变换脱敏

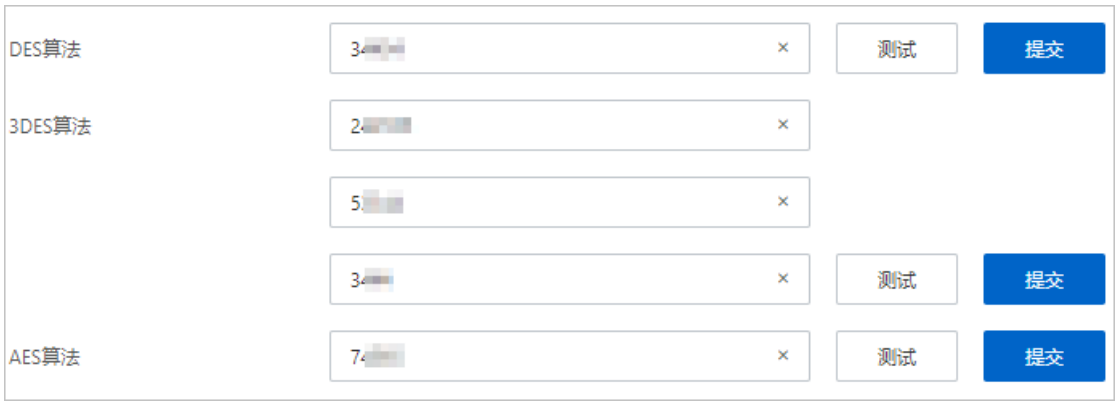
1. 登录云盾安全中心。
2. 在左侧导航栏，选择**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 脱敏算法**。
3. 在左侧导航栏，选择**数据脱敏 > 脱敏算法**，在**脱敏算法**页面单击**变换脱敏**页签。
4. 设置变换脱敏算法的参数。



5. 在**脱敏算法测试**面板，单击**测试**，测试是否脱敏。
6. 测试完成后，单击**提交**。

加密脱敏

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 脱敏算法**。
3. 在左侧导航栏，选择**数据脱敏 > 脱敏算法**，在**脱敏算法**页面单击**加密脱敏**页签。
4. 设置加密脱敏算法的密钥。



5. 在**脱敏算法测试**面板，单击**测试**，测试是否脱敏。
6. 测试完成后，单击**提交**。

洗牌脱敏

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**数据安全 > 敏感数据保护 > 敏感数据脱敏 > 脱敏算法**。
3. 在左侧导航栏，选择**数据脱敏 > 脱敏算法**，在**脱敏算法**页面单击**洗牌脱敏**页签。
4. 选择洗牌脱敏的洗牌方式。



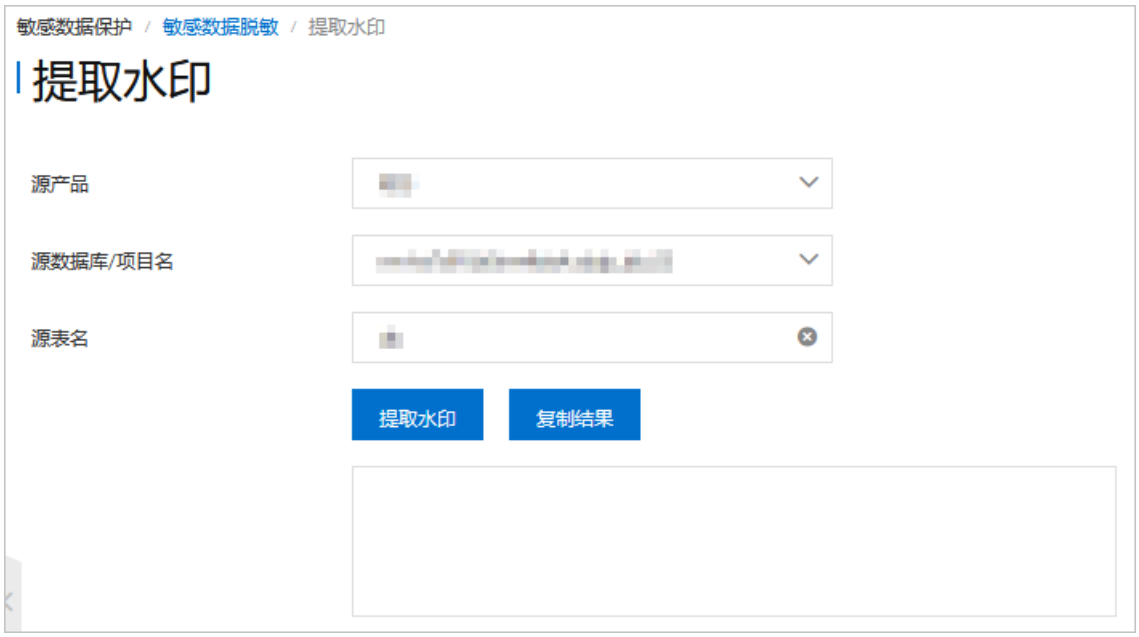
5. 单击**提交**。

10.4.7.5. 提取水印

新增脱敏任务时添加水印后可以使数据分发后实现泄露数据溯源，保证分发数据正常使用。当信息泄露时可以从泄露的数据中提取水印标识，通过读取水印标识，追溯数据流转过程，精准定位泄露单位及责任人，实现数据溯源追责。本文介绍如何提取水印。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**敏感数据脱敏 > 提取水印**。
4. 在**提取水印**页面，选择**源产品**、**源数据库/项目名**，输入**源表名**，单击**提取水印**。



参数	说明
源产品	选择包含水印的表所在的源产品名称。
源数据库/项目名	选择包含水印的表所在的源数据库或项目名称。
源表名	输入水印所在的数据表名称。

提取成功后信息会在页面下方文本框中显示，如需复制信息可单击**复制结果**。

10.4.8. 报表中心

10.4.8.1. 综合分析报告

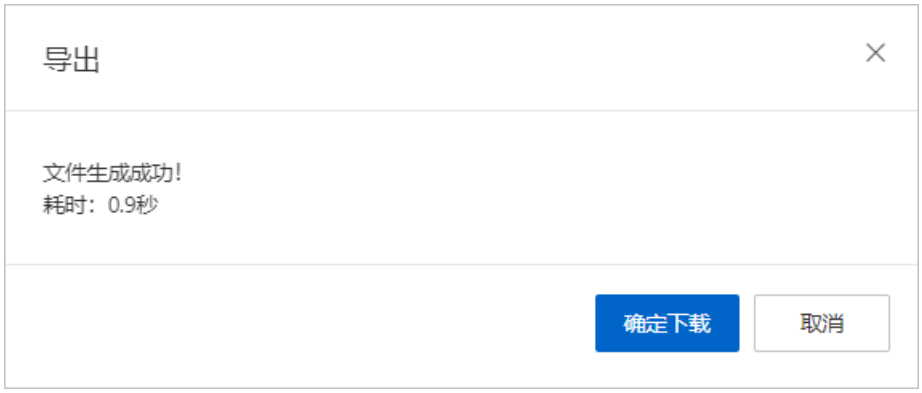
通过资产管理和安全保障、异常和审计事件、敏感数据访问及规则命中和SQL语句执行情况四个角度对数据库进行综合分析，得出总体综合概况报表。本文介绍了如何导出综合分析报告。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**报表中心 > 综合分析报告**。
4. 在**综合分析报告**页面，设置**资产**和**时间范围**。

   您可以在资产列表中，选择您想要导出查看的资产，时间范围可以设置**本日**、**本周**、**本月**、**最近3个月**、**最近6个月**、**最近12个月**、**昨天**、自定义。



5. 单击**导出**。
6. 在**导出**对话框，单击**确定下载**，下载综合分析报告。



10.4.8.2. 等保参考分析报表

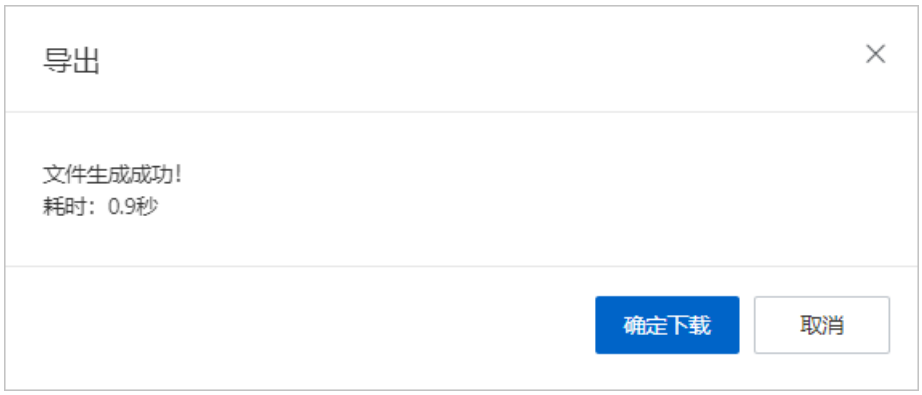
结合网络安全等级保护2.0制度，您可以从数据库审计情况、入侵防范监控、安全审计监控角度，得出资产等保2.0下的风险参考报表。本文介绍如何导出等保参考分析报表。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，选择**报表中心 > 等保参考分析报表**。
4. 在**等保参考分析报表**页面，设置**资产**和**时间范围**。

   您可以在资产列表中，选择您想要导出查看的资产，时间范围可以设置**本日**、**本周**、**本月**、**最近3个月**、**最近6个月**、**最近12个月**、**昨天**、自定义。



5. 单击**导出**。
6. 在**导出**对话框，单击**确定下载**，下载等保参考分析报表。



10.4.9. 新增使用授权

敏感数据保护（SDDP）在使用前，需要为部门进行授权，该章节介绍如何为部门进行授权。

前提条件

在为部门进行授权前，需要先获取部门的名称和AK信息，具体操作请参见 *Apsara Uni-manager运营控制台用户指南*的**企业中心 > 组织管理 > 获取组织AccessKey**章节。

背景信息

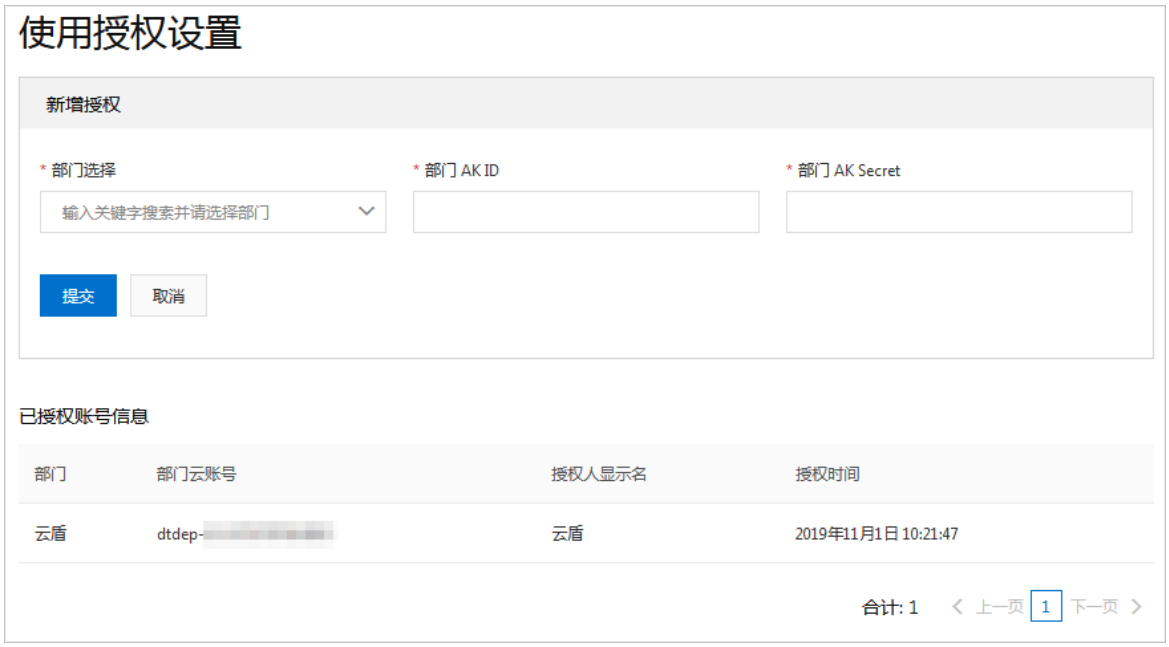
SDDP在使用前，需要为部门进行授权：

- 安全管理员在使用SDDP前，需要先为自己用户所在的部门进行授权。
- SDDP在检测敏感数据之前，需要先获取数据所属的部门授权，授权SDDP允许访问部门各产品（MaxCompute、OSS、ADS和OTS）的数据。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 敏感数据保护**。
3. 在左侧导航栏，单击**使用授权**。

> **说明** 如果用户所在部门未进行授权，在进入敏感数据保护时，直接进入**使用授权设置**页面。



4. 在**新增授权**区域，新增部门授权。
   i. 在**部门选择**中，输入部门关键字，并选择部门。
   ii. 输入**部门AK ID**和**部门AK Secret**信息。
   iii. 单击**提交**，新增部门授权。
5. 在**已授权账号信息**区域，查看已授权的部门列表。

10.5. 数据梳理

10.5.1. 快速部署指南

10.5.1.1. 部署数据梳理系统

该章节介绍如何在云盾安全中心部署数据梳理系统。

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。

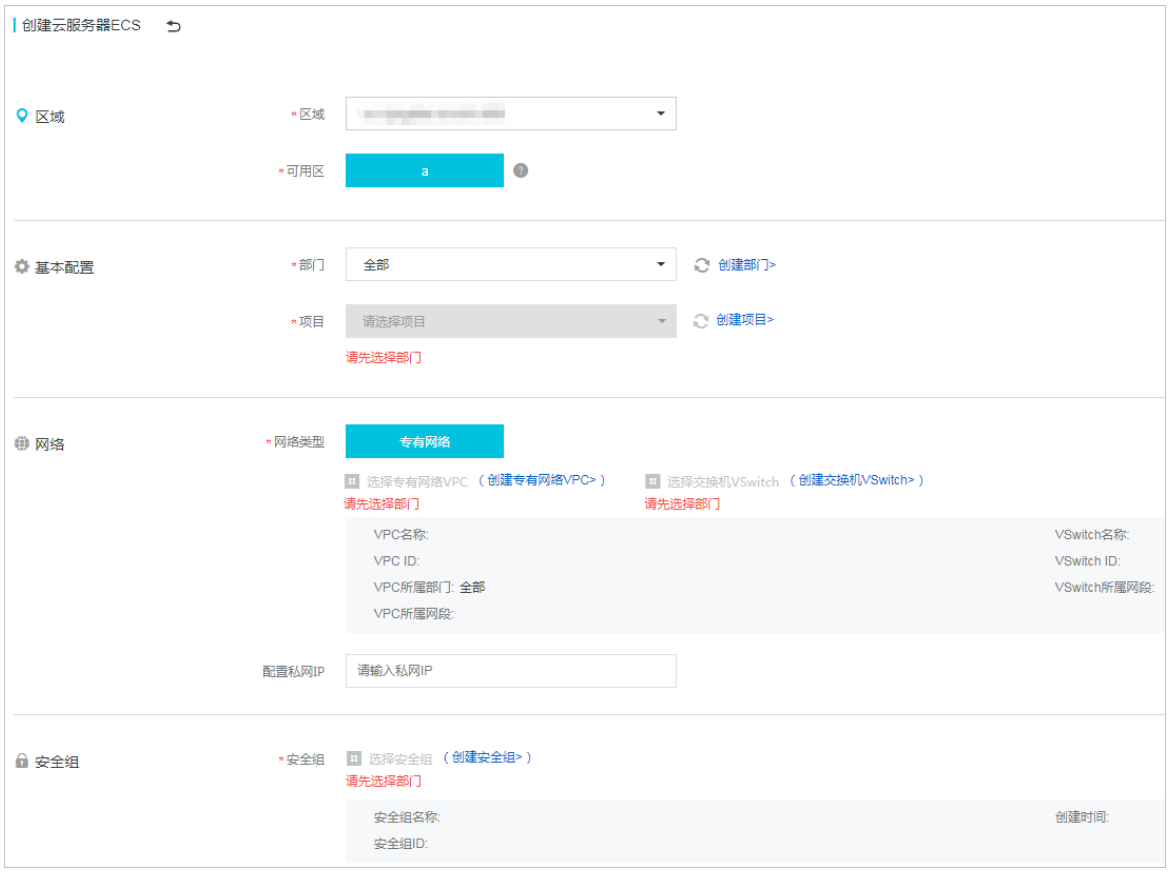
背景信息

数据梳理系统通过镜像方式部署在服务器中。通过数据梳理系统，发现数据库、识别敏感数据和梳理数据库权限。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，单击**数据安全 > 数据梳理**

3. 单击**我要创建**，进入**云服务器ECS**页面。
4. 单击**实例**页签，单击**创建实例**。
5. 在**创建云服务器ECS**页面，创建数据梳理系统服务器。



   i. 设置区域、配置基本配置、网络等信息。
   ii. 单击**选择实例规格**，选择4核12 G类型的ECS实例规格。

   > **说明** 数据梳理系统必须使用4核12 G或以上的实例规格。

   iii. 选择公共镜像，选择云盾数据梳理系统镜像，并选择对应的版本。
   iv. 添加一块100 GB的系统盘。
   v. 填写服务器密码、实例名称，单击**创建**，创建数据梳理系统。
6. 联系销售人员，申请数据梳理系统正式版的License许可。

10.5.1.2. 配置自定义IP

本文介绍如何配置数据梳理系统的自定义IP。

背景信息

云盾用户通过自定义IP，可以在云盾安全中心直接访问数据梳理系统。

操作步骤

1. 登录Apsara Uni-manager运营控制台。

具体步骤请参见登录云盾安全中心。

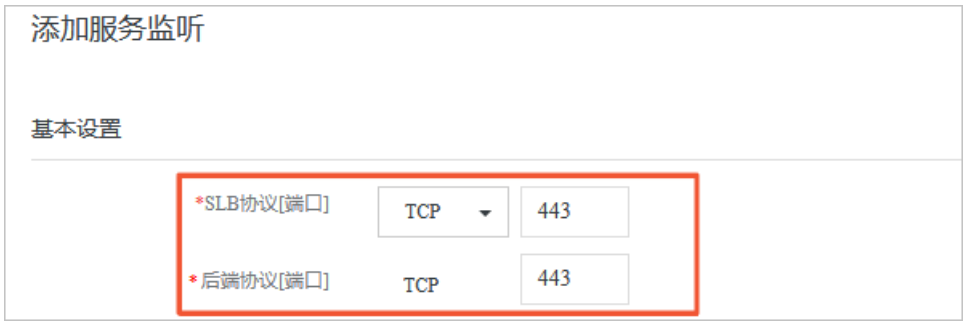
2. 创建数据梳理系统的SLB服务。

   具体步骤，请参见 *负载均衡用户指南*的**创建负载均衡实例**章节，创建负载均衡实例。

   > 说明
   >
   > 记录下SLB的服务地址，该地址即数据梳理系统的自定义IP。

   其中，SLB的**服务监听**和**后端服务器**配置如下：

   - **服务监听**：设置TCP协议和443端口，如下图所示。

   - **后端服务器**：选择数据梳理系统的服务器。

3. 登录云盾安全中心。
4. 在左侧导航栏，选择**数据安全 > 数据梳理**。
5. 在云盾数据梳理系统的**操作**栏，单击**管理**。
6. 在**管理**对话框中，单击**新增自定义访问地址**。
7. 输入SLB的服务地址，单击**保存**。

10.5.1.3. 登录数据梳理系统（云盾安全中心登录）

该章节介绍如何在云盾安全中心直接登录数据梳理系统。

背景信息

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。

操作步骤

1. 登录云盾安全中心。
2. 单击**数据安全 > 数据梳理**。
3. 在需要登录数据梳理系统的**操作**栏，单击**管理**，查看登录信息。
4. 单击**自定义**后面的IP地址，登录到数据梳理系统。

10.5.1.4. 导入许可证

该章节介绍如何在数据梳理系统中导入许可证。

背景信息

安装系统后，数据梳理系统为试用状态，只有导入正式版License文件，系统才能够正常工作。

操作步骤

1. 登录数据梳理系统。
2. 单击**开启密码登录**。
3. 输入sysadmin用户的密码，单击**确定**。
4. 单击**退出**，退出当前用户。
5. 输入sysadmin和设置的密码，单击**登录**。
6. 在**上传证书文件**右侧，单击 。
7. 选择本地正式版的License文件，单击 。

执行结果

上传成功后，即可以正式使用数据梳理系统。

10.5.2. 数据源管理

10.5.2.1. 创建数据库发现任务

该章节介绍如何创建数据库发现任务。

背景信息

通过指定IP段和端口的范围，自动搜索发现网内数据库。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库发现任务**。
3. 在**任务列表**中，单击右上角的 。
4. 设置数据库发现任务参数。
   i. 设置数据库发现任务的基本信息。

设置项	说明
任务名称	自定义数据库发现任务的任务名称。
网卡	在下拉菜单中选择网卡。
描述	描述数据库发现任务。

   ii. 设置数据库发现任务的IP网段，单击**添加到IP列表**。

   数据库发现任务自动发现该网段的数据库，IP网段需要和**基本信息**中设置的**网卡**对应。

   添加成功后，IP段将显示在**已添加IP段**区域。

iii. 设置数据库的端口范围，单击 ＋ 。

- 系统中已经列出常用数据库的默认端口，如果您数据库自定义了端口号，需要修改为自定义的端口范围。
- 如果需要添加所有数据库类型，单击**全部添加**。

添加成功后，端口范围将显示在**已添加端口范围**区域。

iv. 验证主机是否存在配置。

5. 单击右上角的 ，创建数据库发现任务。

10.5.2.2. 执行数据库发现任务

该章节介绍如何执行数据库发现任务。

背景信息

通过执行数据库发现任务，自动发现内部的数据库信息。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库发现任务**。
3. 在**任务列表**中，单击发现任务**操作**栏中的 **> 启动任务**。

10.5.2.3. 管理数据库发现任务

该章节介绍如果管理数据库发现任务。

背景信息

数据梳理系统支持停止任务、查看/编辑任务、查看任务执行详情、设置定时任务等操作。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库发现任务**。
3. 在**任务列表**中，管理数据库发现任务。
   - **停止任务**

     对于正在执行的任务，单击 **> 停止任务**，停止数据库发现任务。
   - **查看/编辑任务**

     单击 **> 查看/编辑任务**，查看和编辑数据库发现任务。
   - **任务执行详情**

     单击 **> 任务执行详情**，查看数据库发现任务执行的详情。
   - **设置定时任务**

如果需要定时启动数据库发现任务，可以参考以下操作。

a. 单击 > **设置定时任务**。

b. 设置定时任务参数。



c. 单击 。

10.5.2.4. 添加数据源

该章节介绍如何添加数据源。

背景信息

通过数据库发现功能，可以自动发现数据库。同时，也可以在数据源中手动添加数据库。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据源**。
3. 在**数据源列表**中，单击右上角的 。
4. 在**添加数据源**中，设置数据源相关参数。



5. 单击**测试连接**，测试是否成功连接该数据库。
6. 测试成功后，单击**确定**，完成添加数据源操作。

10.5.2.5. 查询数据源

该章节介绍如何查询数据源。

背景信息

通过查询数据源操作，快速定位和查看数据源信息。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据源**。
3. 在**数据源列表**区域，查看所有的数据源信息。
4. 在**查询条件**区域，设置查询条件，单击**查询**。
   在**数据源列表**区域，可以查看查询结果。

10.5.3. 敏感数据任务管理

10.5.3.1. 自定义发现规则

该章节介绍如何自定义发现规则。

背景信息

系统已经内置一些常用的敏感数据发现规则，可以满足一般情况下的敏感数据任务。如果需要更加准确的发现敏感数据，可以根据自身业务特点，自定义发现规则。

操作步骤

1. 登录数据梳理系统。
2. 单击**配置 > 发现规则配置**。
3. 在**发现规则列表**区域，单击 ＋ 。
4. 配置发现规则的参数。



5. 单击 保存 。

10.5.3.2. 创建敏感数据任务

该章节介绍如何创建敏感数据任务。

背景信息

通过敏感数据发现规则，自动发现数据源中的敏感数据。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库扫描任务**。
3. 单击**敏感数据任务**页签。
4. 在**敏感数据任务列表**区域，单击右侧的 ＋ 。
5. 在**创建任务**对话框中，设置敏感数据任务参数。
   i. 在**选择数据源**中，单击 ，选择数据源。

ii. 在**内置发现规则**中，选择系统内置的发现规则。

iii. 在**自定义发现规则**中，选择您自定义的发现规则。

iv. 在**高级配置**中，配置高级参数。

6. 单击**保存**，创建敏感数据任务。

> **说明** 如果单击**保存并执行**，那么保存后将直接执行该任务。

10.5.3.3. 执行敏感数据任务（单任务）

该章节介绍如何执行敏感数据任务。

背景信息

通过执行敏感数据任务，发现数据源中的敏感数据。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库扫描任务**。
3. 单击**敏感数据任务**页签。
4. 在**敏感数据任务列表**区域，单击任务**操作**栏中的 > **运行任务**。

10.5.3.4. 批量执行任务

该章节介绍如何创建任务组，并批量执行任务。

背景信息

除了单个执行任务，也可以通过任务组的形式，批量执行任务。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 批量执行任务**。
3. 在**任务组列表**区域，创建任务组。

   i. 单击右侧的 + 。

   ii. 在**新建任务**页面，输入**任务组名称**和**描述**信息。

   iii. 在右侧的**未添加任务**区域，选中需要批量执行的任务。

   iv. 单击 < ，将任务添加到**已添加任务**区域。

   > **说明** 通过中间的操作按钮，可以调整任务组中的任务。

   v. 单击 ，完成创建任务组操作。

4. 在**查询条件**区域，在**任务组名称**中输入关键字，单击**查询**。

   在**任务组列表**区域，可以查看查询结果。

5. 在**任务组列表**区域，单击任务组**操作**栏中的 > **运行任务**。

   任务组中的各任务将批量执行。

10.5.3.5. 查看敏感数据任务结果

该章节介绍如何查看敏感数据任务执行后的结果。

背景信息

执行敏感数据任务后，可以在扫描任务结果中查看执行结果。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 扫描任务结果**。
3. 在左侧区域，单击**敏感数据任务**页签。
4. 单击某一敏感数据任务，在右侧区域可以查看该任务的执行结果。
5. 在**查询条件**区域中，设置查询条件，单击**查询**
6. 在**发现数据列表**区域中，可以查看查询结果。

10.5.4. 权限梳理任务管理

10.5.4.1. 创建权限梳理任务

该章节介绍如何创建权限梳理任务。

背景信息

通过权限梳理任务，发现数据源中的账户清单。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库扫描任务**。
3. 在**权限梳理任务列表**区域，单击右侧的 + 。
4. 在**创建任务**对话框中，设置权限梳理任务参数。
   i. 在**选择数据源**中，单击 ，选择数据源。
   ii. 设置是否定时执行任务。
5. 单击**保存**，创建权限梳理任务。

> **说明** 如果单击**保存并执行**，那么保存后将直接执行该任务。

10.5.4.2. 执行权限梳理任务（单任务）

该章节介绍如何执行权限梳理任务。

背景信息

通过执行权限梳理任务，发现数据源中的账户清单。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 数据库扫描任务**。
3. 单击**权限梳理任务**页签。
4. 在**权限梳理任务列表**区域，单击任务**操作**栏中的 > **运行任务**。

10.5.4.3. 批量执行任务

该章节介绍如何创建任务组，并批量执行任务。

背景信息

除了单个执行任务，也可以通过任务组的形式，批量执行任务。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 批量执行任务**。
3. 在**任务组列表**区域，创建任务组。
   i. 单击右侧的 + 。
   ii. 在**新建任务**页面，输入**任务组名称**和**描述**信息。
   iii. 在右侧的**未添加任务**区域，选中需要批量执行的任务。
   iv. 单击 < ，将任务添加到**已添加任务**区域。

   > **说明** 通过中间的操作按钮，可以调整任务组中的任务。

   v. 单击 ，完成创建任务组操作。
4. 在**查询条件**区域，在**任务组名称**中输入关键字，单击**查询**。
   在**任务组列表**区域，可以查看查询结果。
5. 在**任务组列表**区域，单击任务组**操作**栏中的 > **运行任务**。
   任务组中的各任务将批量执行。

10.5.4.4. 查看权限梳理任务结果

该章节介绍如何查看权限梳理任务执行后的结果。

背景信息

执行权限梳理任务后，可以在扫描任务结果中查看执行结果。

操作步骤

1. 登录数据梳理系统。
2. 单击**任务管理 > 扫描任务结果**。
3. 在左侧区域，单击**权限梳理任务**页签。
4. 单击某一权限梳理任务，在右侧区域可以查看该任务的执行结果。
5. 在**查询条件**区域中，设置查询条件，单击**查询**。
6. 在**数据库账户清单**区域中，可以查看查询结果。

10.6. 数据发现与脱敏

10.6.1. 快速部署指南

10.6.1.1. 部署数据发现和脱敏系统

该章节介绍如何部署数据发现和脱敏系统。

前提条件

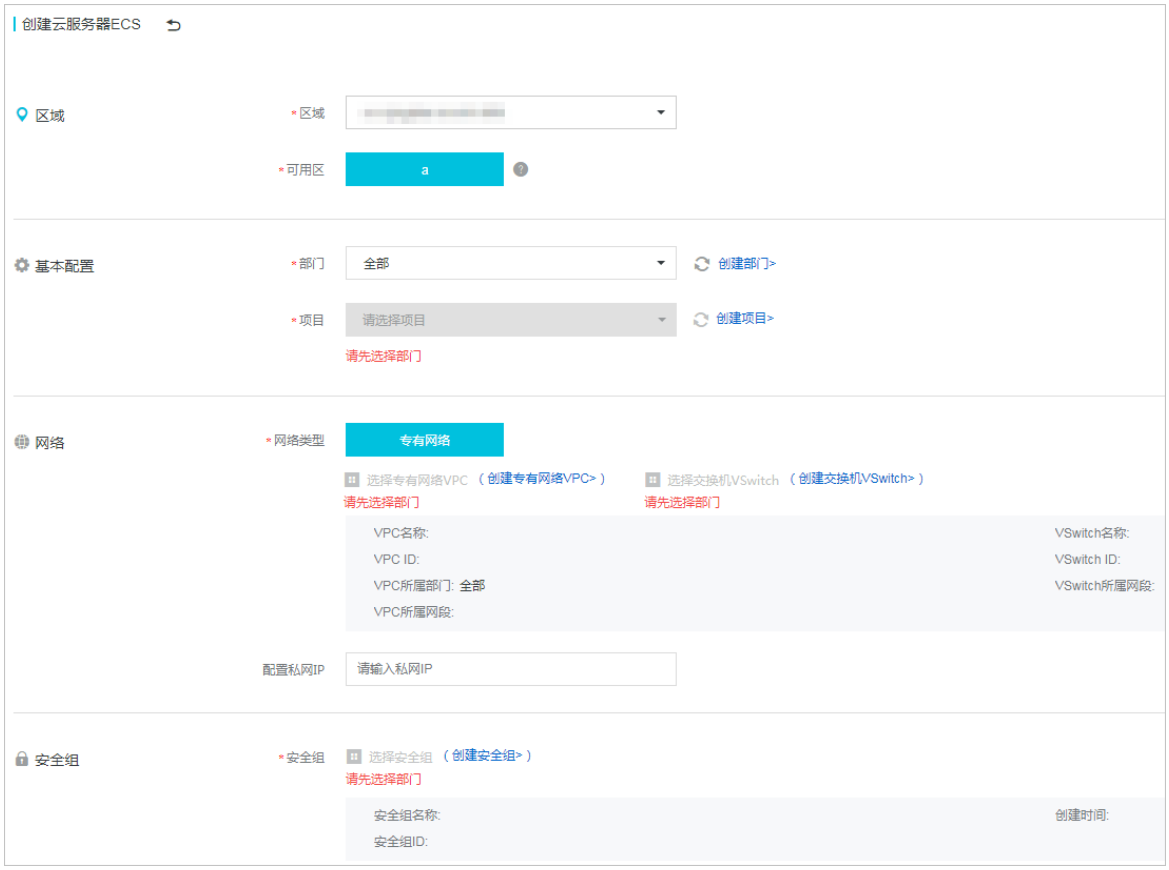
确认您所使用的账号已具备相应部门的云资源权限，例如具备部门管理员角色权限。

背景信息

数据发现和脱敏系统通过镜像方式部署在专有云的服务器中。数据库发现与脱敏系统能够检测发现环境中的数据库，并提供数据脱敏功能。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，单击**数据安全 > 数据发现和脱敏**。
3. 单击**我要创建**，进入**云服务器ECS**页面。
4. 单击**实例**页签，单击**创建实例**。
5. 在**创建云服务器ECS**页面，创建云盾数据发现和脱敏系统服务器。



i. 根据实际情况，设置区域、基本配置和网络等信息。

ii. 单击**选择实例规格**，选择4核12 G类型的ECS实例规格。

> **说明** 云盾数据发现和脱敏系统必须使用4核8 G或以上的实例规格。

iii. 选择**公共镜像**，选择*云盾数据发现脱敏*镜像，并选择对应的版本。

iv. 添加一块100 GB的系统盘和一块至少500 GB的数据盘。

v. 填写服务器密码、实例名称，单击**创建**，创建云盾数据发现和脱敏系统。

6. 联系销售人员，申请云盾数据发现和脱敏系统正式版的License许可。

10.6.1.2. 配置自定义IP

本文介绍如何配置数据发现与脱敏系统的自定义IP。

背景信息

云盾用户通过自定义IP，可以在云盾安全中心直接访问数据发现与脱敏系统。

操作步骤

1. 登录Apsara Uni-manager运营控制台。

   具体步骤，请参见登录云盾安全中心。

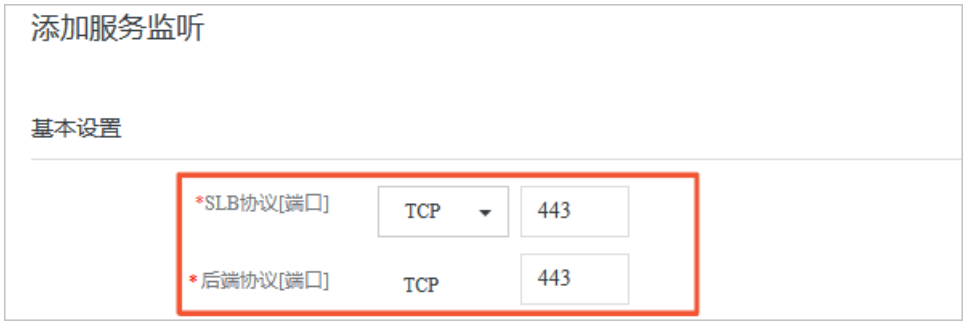
2. 创建数据发现与脱敏系统的SLB服务。

   具体步骤，请参见 *负载均衡用户指南*的**创建负载均衡实例**章节，创建负载均衡实例。

> **说明** 记录下SLB的服务地址，该地址即数据发现与脱敏系统的自定义IP。

其中，SLB的**服务监听**和**后端服务器**配置如下：

- **服务监听**：设置TCP协议和443端口，如下图所示。



- **后端服务器**：选择数据发现与脱敏系统的服务器。

3. 登录云盾安全中心。
4. 在左侧导航栏，选择**数据安全 > 数据发现与脱敏**。
5. 在云盾数据发现与脱敏系统的**操作**栏，单击**管理**。
6. 在**管理**对话框中，单击**新增自定义访问地址**。
7. 输入SLB的服务地址，单击**保存**。

10.6.1.3. 登录数据发现与脱敏系统

该章节介绍如何在云盾安全中心直接登录发现与脱敏系统。

前提条件

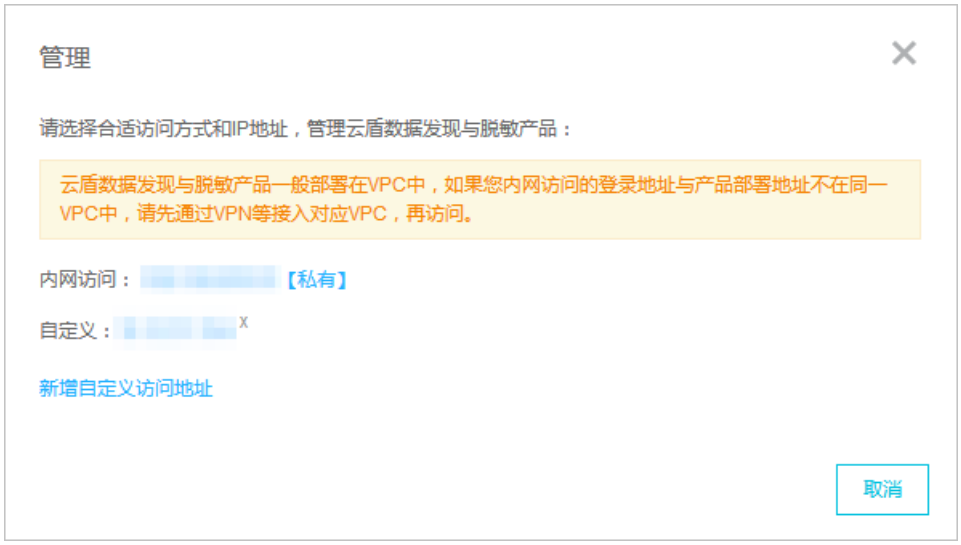
确认您所使用的账号已具备相应部门的云资源权限，例如具备部门管理员角色权限。

背景信息

数据发现与脱敏系统支持用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数据处理操作。

操作步骤

1. 登录云盾安全中心。
2. 单击**数据安全 > 数据发现与脱敏**。
3. 在需要登录数据脱敏系统的**操作**栏，单击**管理**，查看登录信息。



4. 单击**自定义**后面的IP地址，登录到数据脱敏系统。

10.6.1.4. 数据脱敏系统界面

该章节介绍数据脱敏系统界面。

数据脱敏系统的界面主要分为三大区域，功能菜单、数据统计、任务信息，如数据脱敏系统界面所示。

数据脱敏系统界面



各区域详细说明如数据脱敏系统区域说明所示。

数据脱敏系统区域说明

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。

10.6.2. 使用指南

10.6.2.1. 数据源管理

10.6.2.1.1. 数据库

10.6.2.1.1.1. 添加数据库

该章节介绍如何把数据库添加为数据源。

背景信息

数据发现与脱敏系统支持Oracle、MySQL、SQL Server等数据库类型作为数据源。

注意事项：

- 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。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 数据库**。
3. 在**数据库列表**右上角，单击添加按钮。
4. 在**添加数据源**对话框中，设置数据库信息。



5. 单击**测试连接**，测试数据库是否连接成功。

   > **说明** 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。

6. 连接测试成功后，单击**保存**。

10.6.2.1.1.2. 修改数据库

该章节介绍如何在数据源中修改数据库信息。

背景信息

作为数据源的数据库，如果IP、端口、用户等信息发生变更时，可以通过编辑功能修改数据库信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 数据库**。
3. 在**数据库列表**中，单击数据库的按钮。
4. 在**编辑数据源**对话框中，修改数据库信息。

   > **说明** 数据库类型无法修改。

5. 单击**保存**。

10.6.2.1.1.3. 删除数据库

该章节介绍如何在数据源中删除数据库。

背景信息

如果数据库已经不用于数据源，可以通过删除功能删除该数据库信息。

如果数据库信息与数据发现与脱敏系统内其他数据存在关联，将无法删除该数据库信息记录。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。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 数据库**页面。
3. 在**数据库列表**中，单击数据库的按钮。
4. 在**信息提示**对话框中，单击**确定**，删除该数据库信息记录。

10.6.2.1.1.4. 查询数据库

该章节介绍如何查询数据库信息。

背景信息

通过查询功能，快速搜索和查看目标数据库信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 数据库**。
3. 在**数据库列表**中，输入**数据源名称**和**IP**，单击**搜索**。

   > **说明** 数据库搜索功能支持模糊查询。

4. 在查询结果中，单击数据库的按钮，查看详细信息。

10.6.2.1.2. 文件源

10.6.2.1.2.1. 添加文件源

该章节介绍如何添加文件源。

背景信息

数据发现与脱敏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。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**的右上角，单击。
4. 在**添加文件源**对话框中，输入文件源名称和描述。

   > 说明 文件源名称不允许重复。

5. 单击**保存**。

10.6.2.1.2.2. 添加文件

该章节介绍如何在文件源中添加文件。

背景信息

在文件源中添加文件前，需要先通过FTP上传文件到服务器中。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**中，单击文件源**操作**栏中的。
4. 在**文件列表**对话框中，单击。
5. 在**添加文件**对话框中，选择需要添加的文件。



6. 单击**保存**，将该文件添加到文件源中。

> 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。

10.6.2.1.2.3. 修改文件信息

该章节介绍如何修改文件源中的文件配置信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**中，单击文件源**操作**栏中的。
4. 在**文件列表**对话框中，单击文件**操作**栏中的。
5. 在**编辑文件**对话框中，修改该文件的相关设置信息。

   > 说明 在**编辑文件**对话框中，文件源名称及文件名称无法修改。

6. 单击**保存**。

10.6.2.1.2.4. 删除文件

该章节介绍如何删除文件源中的文件。

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。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**中，单击文件源**操作**栏中的。
4. 在**文件列表**对话框中，单击文件**操作**栏中的。
5. 在**信息提示**对话框中，单击**确定**，删除该文件。

10.6.2.1.2.5. 修改文件源

该章节介绍如何修改文件源信息。

背景信息

如果文件源有需要补充描述，可以通过修改文件源功能，修改描述信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**中，单击文件源的按钮。
4. 在**编辑文件源**对话框中，修改文件源的描述信息。
5. 单击**保存**。

10.6.2.1.2.6. 删除文件源

该章节介绍如何删除文件源。

前提条件

删除文件源前，请确认该文件源记录与数据发现与脱敏系统内其他数据已无关联。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**中，单击文件源的按钮。
4. 在**信息提示**对话框中，单击**确定**，删除该文件源。

10.6.2.1.2.7. 查询文件源

该章节介绍如何查询文件源信息。

背景信息

通过查询功能，快速搜索和查看目标文件源信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据源 > 文件源**。
3. 在**文件源列表**中，输入**文件源名称**，单击**搜索**。

   > **说明** 文件源搜索功能支持模糊查询。

4. 在查询结果中，单击文件源的按钮，查看详细信息。

10.6.2.2. 数据发现

10.6.2.2.1. 发现任务

10.6.2.2.1.1. 数据库发现任务

添加数据库发现任务

该章节介绍如何添加数据库类型的发现任务。

背景信息

数据发现：根据指定的部分敏感数据特征或预定义的敏感数据特征，在执行任务过程中对抽取的数据进行自动的识别，发现敏感数据。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现任务**。
3. 单击添加按钮，打开**添加发现任务**对话框。
4. 在**基本信息**中，设置发现任务的基本信息，单击**下一步**。

配置项	说明
任务名称	输入发现任务的名称。 说明 任务名称不可重复。
任务类型	选择**数据库**类型。
数据库	选择发现任务的目标数据库。

5. 在**数据配置**中，配置数据库信息。
   i. 在**当前选择的数据源**中，配置数据库的用户名和密码。
   ii. 单击**连接**，测试数据库是否连通。
   测试连接成功后，在右侧查看该数据库下的数据表。
   iii. 在**数据源浏览**中，选中数据表。
   iv. 单击**下一步**。
6. 在**规则配置**中，设置发现规则，单击**下一步**。
   选择发现任务的发现规则，支持系统内置发现规则和自定义发现规则。

   说明 关于发现规则的具体介绍请参见发现规则。

7. 在**采样配置**中，设置采样规则，单击**保存**，即可完成数据库发现任务的添加。
   采样规则举例：
   - 假设数据库表中有10000行数据，采样前1000行，则一共会抽取1000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，则一共会抽取800行数据进行发现规则验证。

查看数据库发现任务

该章节介绍如何查看数据库发现任务的详细信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现任务**。
3. 在**发现任务名称**列，单击发现任务的名称。
4. 在**发现任务详情**页面，查看该数据库发现任务的详细信息。

执行数据库发现任务

该章节介绍如何运行数据库类型的发现任务。

背景信息

通过发现任务，检测该任务数据源中是否包含有敏感数据信息。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现任务**。
3. 在数据库发现任务的**操作**栏，单击 > **运行任务**。
4. 在**运行发现任务**对话框中，输入数据库的用户名和密码。
5. 单击**检测**，检测数据库是否连通。
6. 检测通过后，单击**运行**，该数据库发现任务即开始执行。

停止数据库发现任务

该章节介绍如何停止数据库类型的发现任务。

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. 登录数据安全控制台。
2. 单击**数据发现 > 发现任务**。
3. 在数据库发现任务的**操作**栏，单击 > **停止任务**，即可终止正在执行的发现任务。

编辑数据库发现任务

该章节介绍如何编辑数据库发现任务。

背景信息

如果数据库发现任务的数据源、发现规则、采样数据需要变动，可参考本章节进行修改。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现任务**。
3. 在数据库发现任务的**操作**栏，单击 > **编辑任务**。
4. 在**编辑发现任务**对话框中，编辑发现任务。

> 说明 任务名称、任务类型、和数据库无法修改，支持修改**数据配置**、**规则配置**和**采样配置**。

5. 单击**保存**。

删除数据库发现任务

该章节介绍如何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。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现任务**。
3. 在数据库发现任务的**操作**栏，单击 > **删除任务**。
4. 在**信息提示**对话框中，单击**确定**，删除该数据库发现任务。

查看数据库发现任务的历史记录

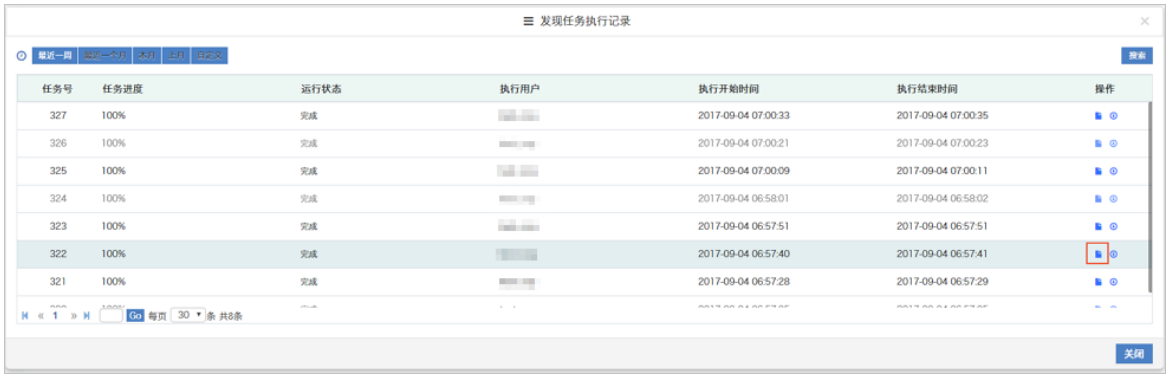
本文介绍如何查看数据库发现任务的历史记录。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，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**。



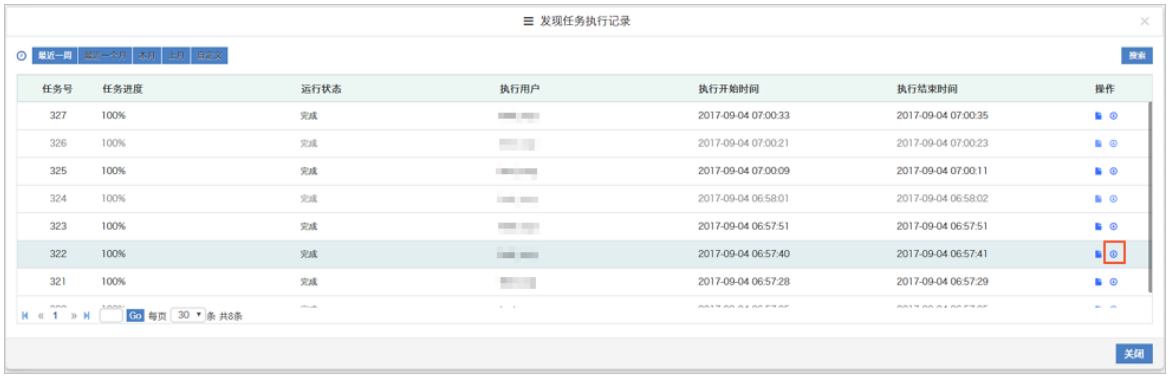
3. 在**发现任务执行记录**对话框中，选择任务记录，单击右侧的执行报告按钮。



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。



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，可将该发现任务的执行日志下载到本地。



10.6.2.2.1.2. 文件发现任务

添加文件发现任务

本文介绍如何添加文件发现任务。

操作步骤

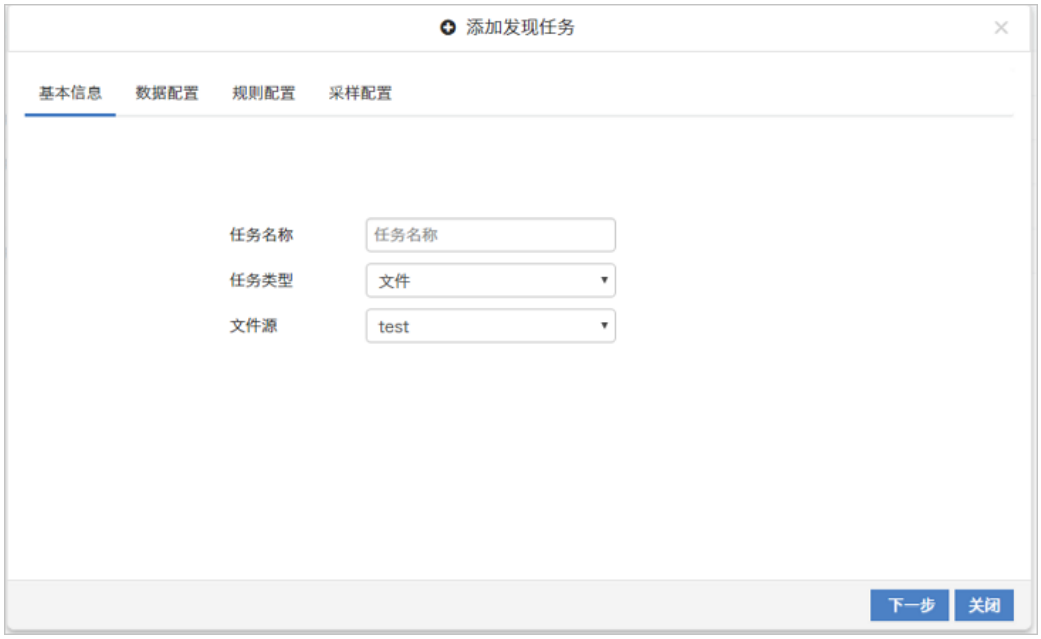
1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，单击**添加**，如发现任务列表所示。

   发现任务列表



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**，如添加发现任务基本信息页签所示。

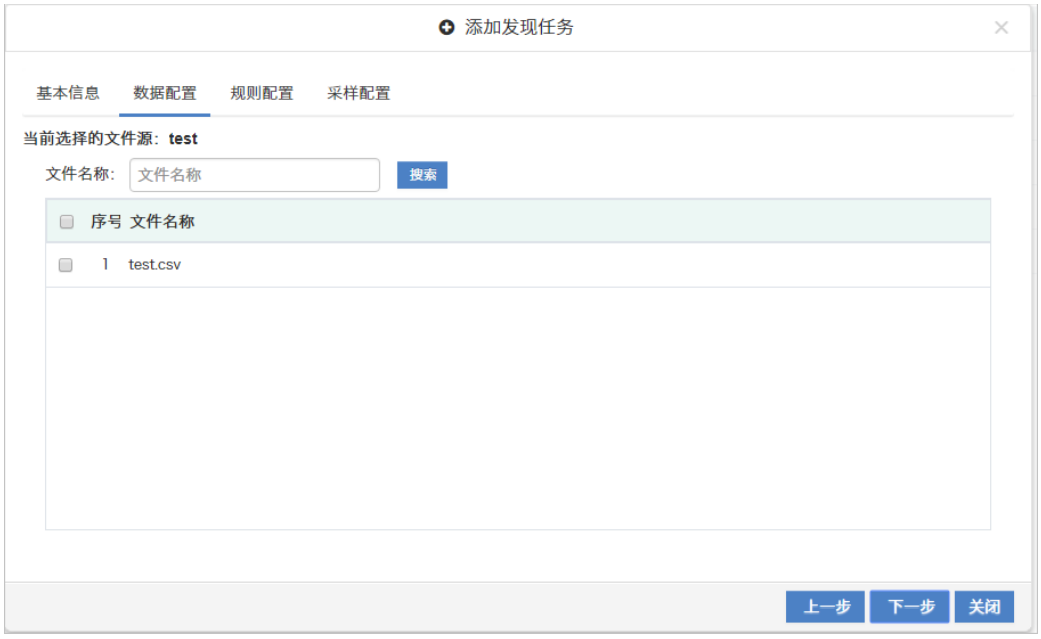
   添加发现任务基本信息页签



> **说明** 任务名称不可重复。

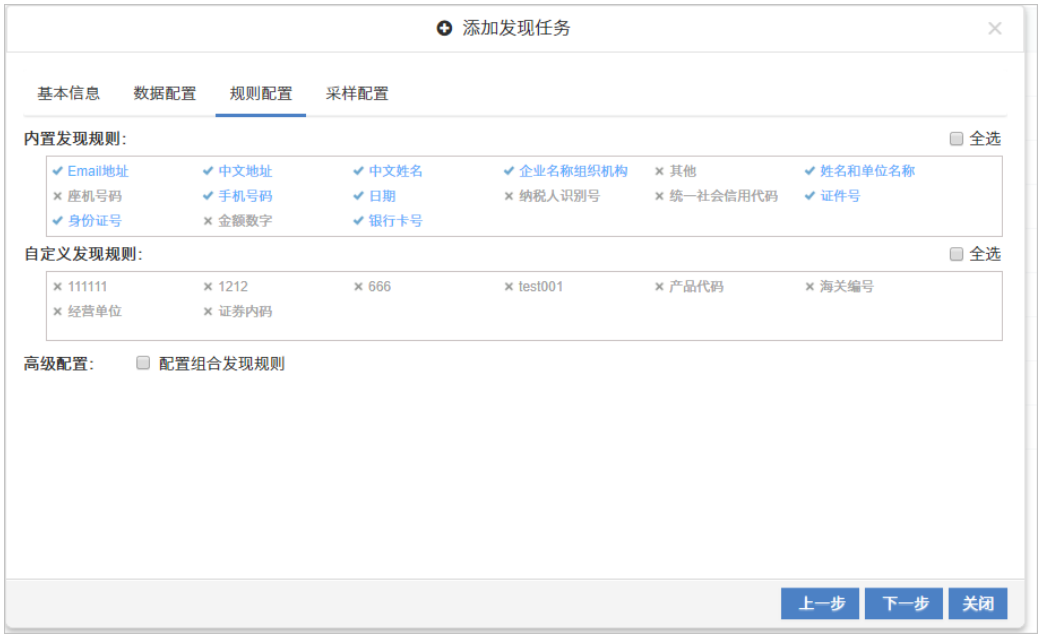
4. 在**添加发现任务**对话框的**数据配置**页签中，选中您想要执行发现任务的文件，单击**下一步**，如添加发现任务数据配置页签所示。

   添加发现任务数据配置页签



5. 在**规则配置**页签中，选择发现规则，单击**下一步**，如添加发现任务规则配置页签所示。

   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。

   添加发现任务采样配置页签



> **说明** 关于发现规则的具体介绍，请参见发现规则。

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。

执行文件发现任务

本文介绍如何执行文件发现任务。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，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**，如发现任务列表所示。

   发现任务列表



3. 在**运行发现任务**对话框中，单击**检测**，如运行发现任务所示。

   运行发现任务



4. 检测通过后，单击**运行**，该文件发现任务即开始执行。

停止文件发现任务

本文介绍如何停止文件发现任务。

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：

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，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**，如停止文件发现任务所示，即可终止正在执行的发现任务。

   停止文件发现任务



查看文件发现任务的历史记录

本文介绍如何查看文件发现任务的历史记录。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，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**，如发现任务列表所示。

   发现任务列表



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，如发现任务执行记录所示。

   发现任务执行记录



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，如发现任务执行报告所示。

   发现任务执行报告



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。

   下载执行日志



编辑文件发现任务

本文介绍如何编辑文件发现任务。

操作步骤

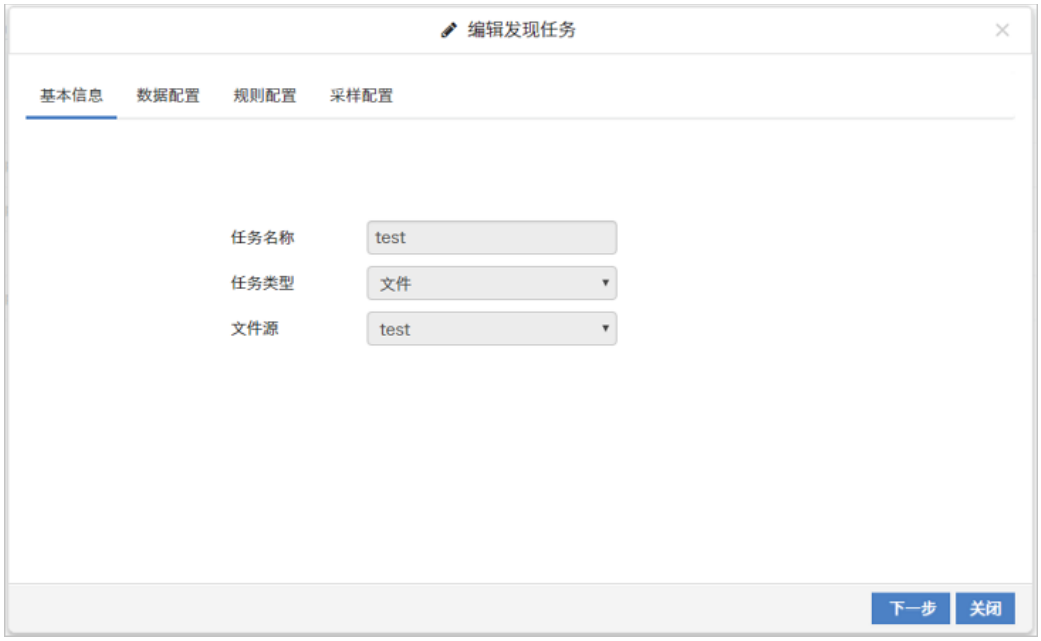
1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，选择已添加的文件发现任务，单击任务记录右侧的操作列表，单击**编辑任务**，如发现任务列表所示。

   发现任务列表



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**，如编辑发现任务所示。

   编辑发现任务



> 说明 任务名称、任务类型、和文件源无法修改。

查看文件发现任务

本文介绍如何查看文件发现任务。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，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，如发现任务详情页面所示。

发现任务详情页面



删除文件发现任务

本文介绍如何删除文件发现任务。

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. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，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**，如删除发现任务所示。

   删除发现任务



3. 在**信息提示**对话框中，单击**确定**，删除该文件发现任务。

10.6.2.2.1.3. 查询发现任务

本文介绍如何查询发现任务。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 发现任务**，选择运行状态，输入发现任务名称，单击**搜索**，如查询发现任务所示，查询包含所设定条件的发现任务。

   查询发现任务



10.6.2.2.2. 敏感字段梳理

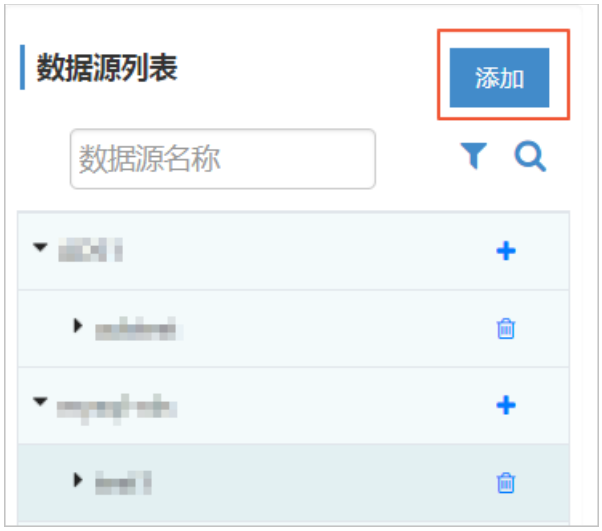
10.6.2.2.2.1. 添加敏感数据源

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。

操作步骤

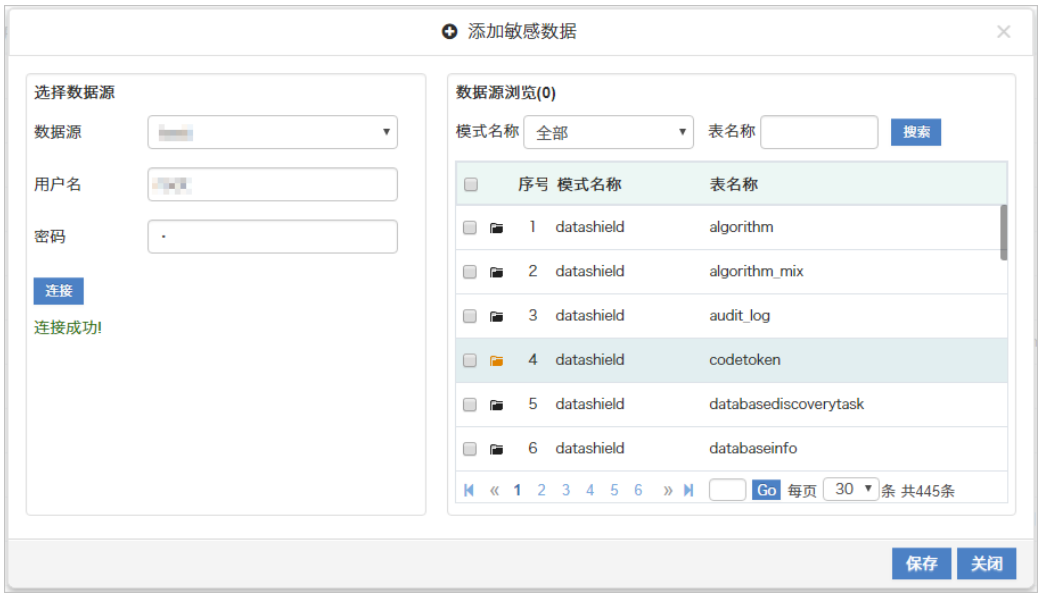
1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感字段梳理**，在数据源列表区域，单击**添加**，如数据源列表所示。

   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**，如新增敏感数据所示。

   新增敏感数据



> **说明** 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。

4. 选中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。

10.6.2.2.2.2. 核实敏感数据

本文介绍如何核实敏感数据。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感字段梳理**，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，如核实敏感数据记录所示，核实该敏感数据。

核实敏感数据记录



- 单击敏感数据列表区域上方的核实当前页按钮，如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。

  核实当前页敏感数据记录



10.6.2.2.2.3. 设置为非敏感数据

本文介绍如何设置为非敏感数据。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感字段梳理**，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，如设置为非敏感数据所示。

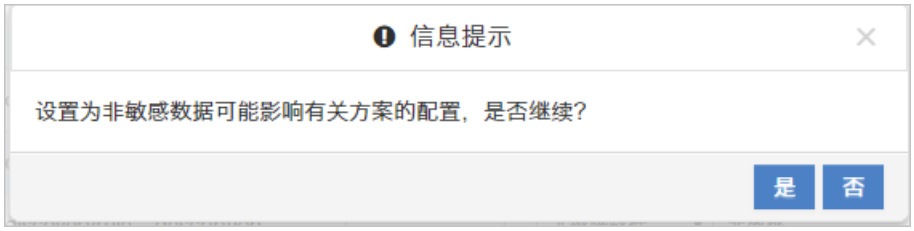
   > **说明** 在敏感级别栏中已标识为非敏感的数据记录无法设置为非敏感数据。

   设置为非敏感数据



3. 在**信息提示**对话框中，单击**是**，如设置非敏感数据信息提示所示。

   设置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。

10.6.2.2.2.4. 修正敏感数据

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。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感字段梳理**，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，如敏感数据列表所示。

   敏感数据列表



3. 在**修正敏感数据**对话框中，修正该敏感数据记录，如修正敏感数据所示。
   - 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。

     修正敏感数据



10.6.2.2.2.5. 查询敏感数据

本文介绍如何查询敏感数据。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感字段梳理**页面，单击**展开更多条件**，如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。

     搜索敏感数据记录



10.6.2.2.3. 敏感文件梳理

10.6.2.2.3.1. 核实敏感数据

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。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感文件梳理**，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，如核实敏感数据记录所示，核实该敏感数据。

     核实敏感数据记录



- 单击敏感文件列表区域上方的核实当前页按钮，如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。

  核实当前页敏感数据记录



10.6.2.2.3.2. 设置为非敏感数据

本文介绍如何将已发现的敏感数据记录设置为非敏感数据。

操作步骤

1. 登录数据安全控制台。
2. 选择**数据发现 > 敏感文件梳理**，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，如设置为非敏感数据所示。

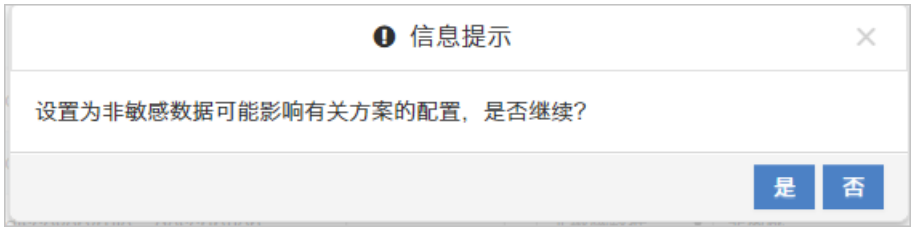
   > **说明** 在敏感级别栏中已标识为非敏感的数据记录无法设置为非敏感数据。

   设置为非敏感数据



3. 在**信息提示**对话框中，单击**是**，如设置为非敏感数据信息提示所示。

   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。

10.6.2.2.3.3. 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. 登录数据安全控制台。
2. 单击**数据发现 > 敏感文件梳理**，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，如敏感文件列表所示。

   敏感文件列表



3. 在**修正敏感数据**对话框中，修正该敏感数据记录，如修正敏感数据所示。
   - 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。

     修正敏感数据



10.6.2.2.3.4. 查询敏感数据

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 敏感文件梳理**，单击**展开更多条件**，如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。

     搜索敏感数据记录



10.6.2.2.4. 发现规则

10.6.2.2.4.1. 查看发现规则

背景信息

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。

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现规则**，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，如查看发现规则所示。

   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。

10.6.2.2.4.2. 添加自定义发现规则

操作步骤

1. 登录数据安全控制台。
2. 单击**数据发现 > 发现规则**，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**，如添加发现规则所示。

   添加发现规则



10.6.2.3. 数据脱敏

10.6.2.3.1. 数据子集

10.6.2.3.1.1. 添加数据子集

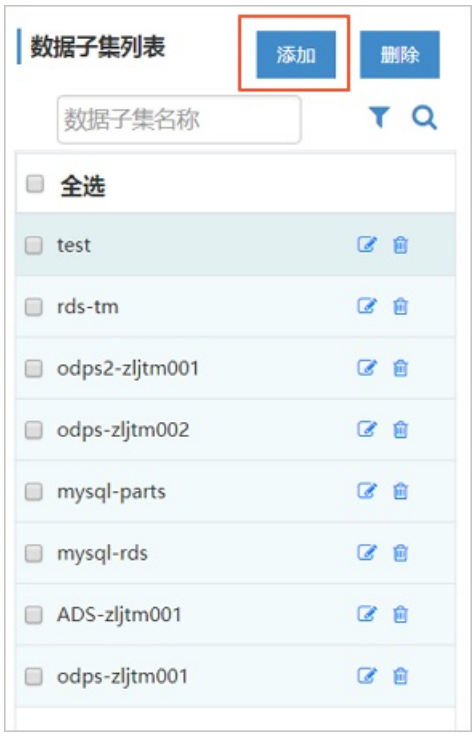
背景信息

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。

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 > 数据子集** 页面，单击左侧数据子集区域的**添加**，如数据子集列表所示。

   数据子集列表



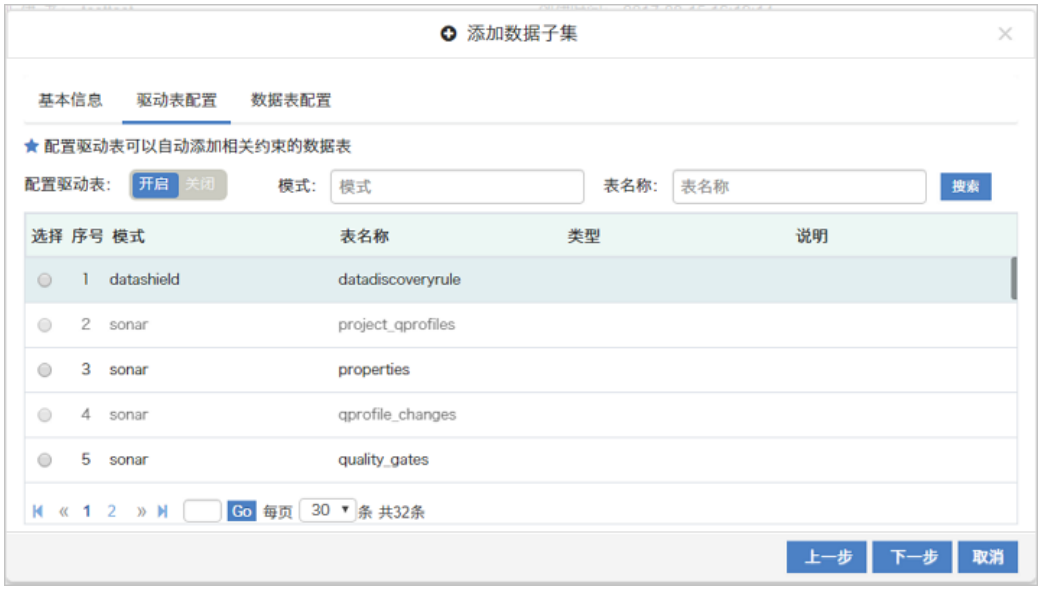
3. 在**添加数据子集**对话框的**基本信息**页签，输入子集名称、数据源、描述，单击**下一步**，如添加数据子集基本信息所示。

   添加数据子集基本信息



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**，如添加数据子集驱动表配置所示。

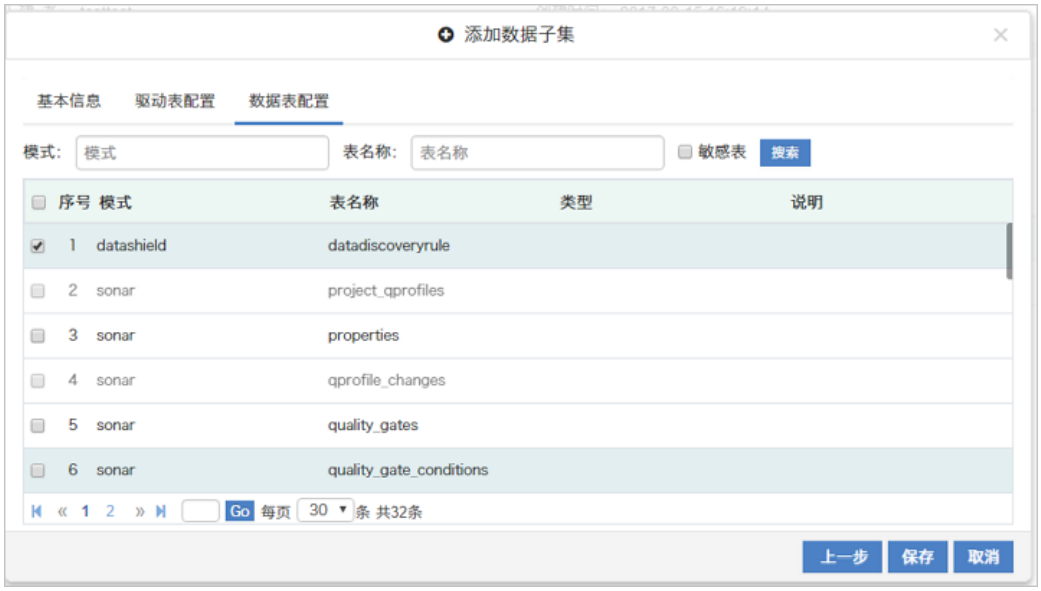
添加数据子集驱动表配置



说明 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**，如添加数据子集数据表配置所示。

添加数据子集数据表配置

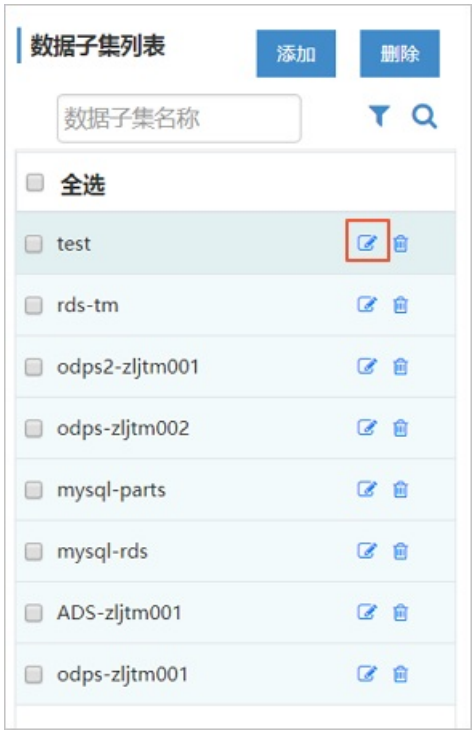


10.6.2.3.1.2. 编辑数据子集

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，如数据子集列表所示。

数据子集列表



2. 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，如编辑数据子集信息所示。

   编辑数据子集信息



> 说明 数据子集的数据源无法修改。

10.6.2.3.1.3. 删除数据子集

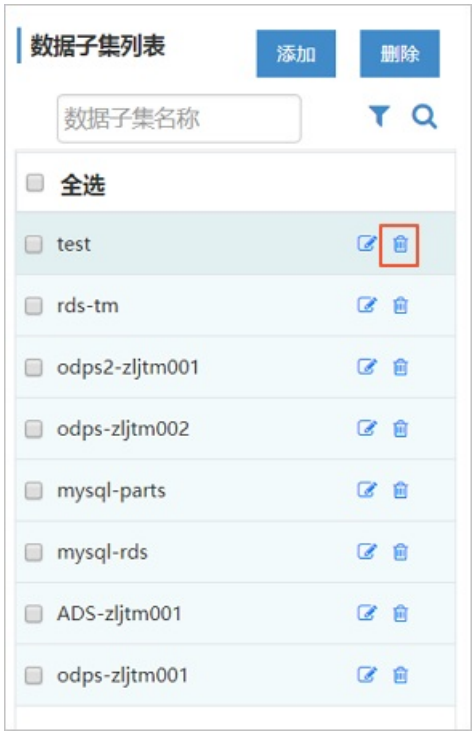
前提条件

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。

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 > 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，如数据子集列表所示。

   数据子集列表



3. 在**信息提示**对话框中，单击**确定**删除该数据子集。

10.6.2.3.2. 数据关系

10.6.2.3.2.1. 查看数据关系

背景信息

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。

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 > 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，如数据关系所示。

   数据关系



10.6.2.3.3. 脱敏方案

10.6.2.3.3.1. 添加数据库脱敏方案

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**，如方案列表所示。

   方案列表



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**，如添加方案基本信息所示。

   添加方案基本信息

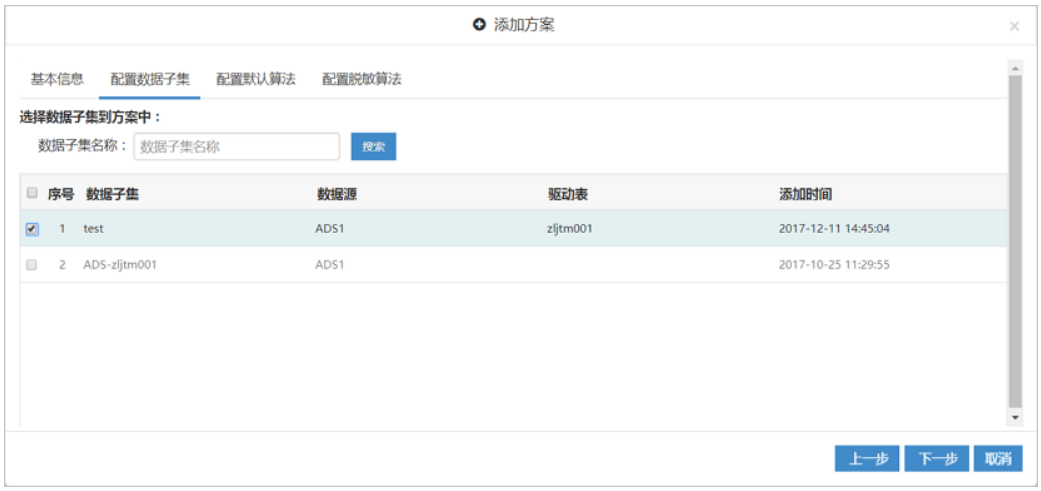


> **说明** 脱敏方案名称不可重复。

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**，如添加方案配置数据子集所示。

> **说明** 输入数据子集名称，单击**搜索**，可查询相应的数据子集。

添加方案配置数据子集



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。

添加方案配置默认算法



6. 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**，如添加方案配置脱敏算法所示，完成添加脱敏方案。

   添加方案配置脱敏算法



10.6.2.3.3.2. 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**，如方案列表所示。

   方案列表



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**，如添加方案基本信息所示。

   添加方案基本信息



> **说明** 脱敏方案名称不可重复。

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。

   添加方案配置默认算法



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**，如添加方案配置脱敏算法所示，完成添加脱敏方案。

   添加方案配置脱敏算法



10.6.2.3.3.3. 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，如方案列表所示。

   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**，如编辑脱敏方案所示。

   编辑脱敏方案



10.6.2.3.3.4. 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，如删除脱敏方案所示。

   删除脱敏方案



4. 在**信息提示**中，单击**确定**。

10.6.2.3.4. 脱敏任务

10.6.2.3.4.1. 数据库脱敏任务

添加数据库脱敏任务

背景信息

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。

操作步骤

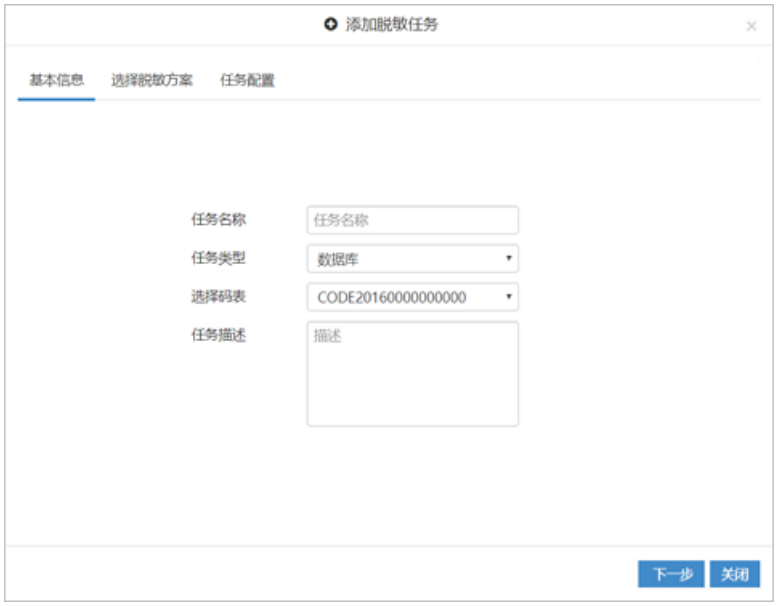
1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏 > 脱敏任务**页面，单击右上角的**添加**，如脱敏任务列表所示。

   脱敏任务列表



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**，如添加脱敏任务基本信息所示。

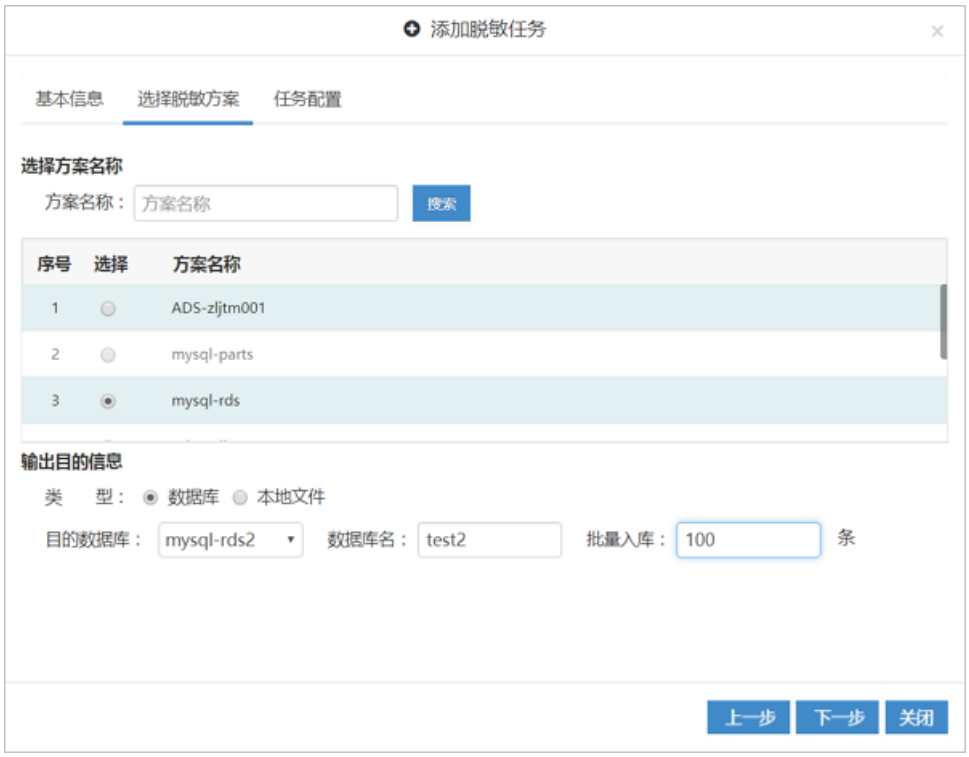
   添加脱敏任务基本信息



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**，如选择脱敏方案所示。

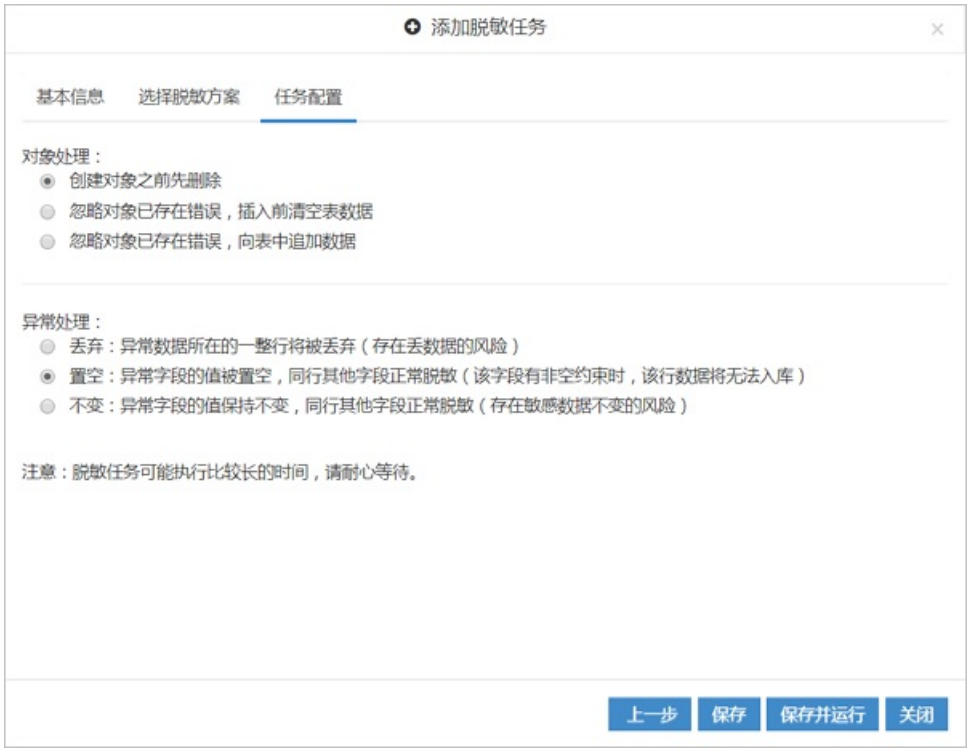
> **说明** 输出目的数据库的schema不能与数据库源的schema相同。

选择脱敏方案



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，如脱敏任务配置所示，单击**保存**，完成该脱敏任务的添加。

脱敏任务配置



执行数据库脱敏任务

操作步骤

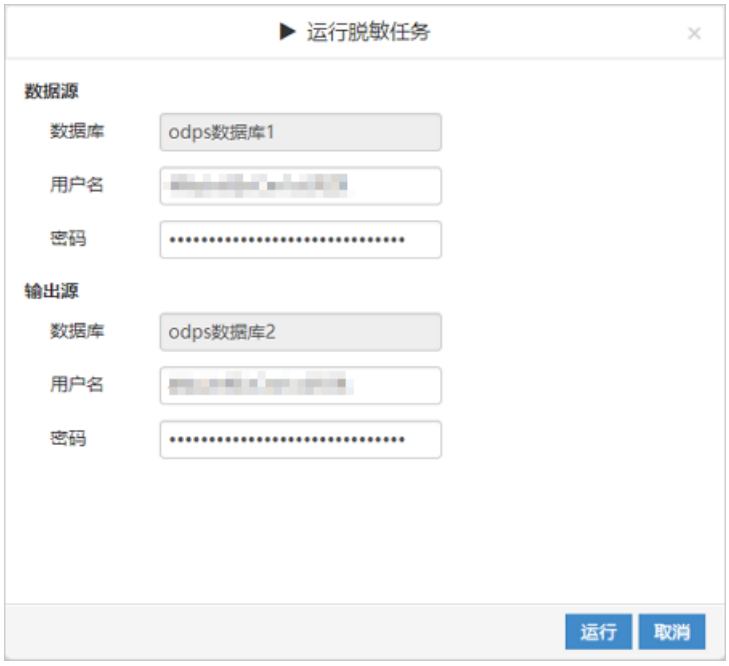
1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏 > 脱敏任务**页面，在**脱敏任务列表**中选择已添加的数据库脱敏任务，单击任务记录右侧的操作列表，单击**运行任务**，如脱敏任务列表所示。

   脱敏任务列表



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，如运行脱敏任务所示。

   运行脱敏任务



等待该数据库脱敏任务执行完毕，如脱敏任务运行完成所示。

脱敏任务运行完成



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。
2. 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**，如停止脱敏任务所示。

   停止脱敏任务



3. 在**信息提示**对话框中，单击**确定**。

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。
2. 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

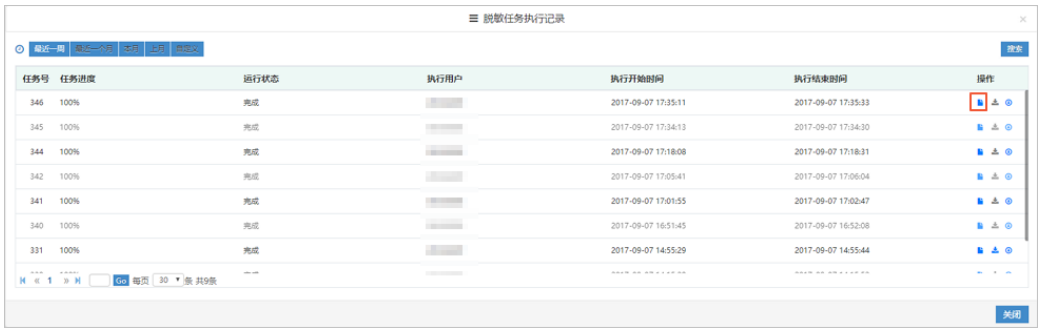
侧的操作列表，单击**历史任务**，如脱敏任务列表所示。

脱敏任务列表



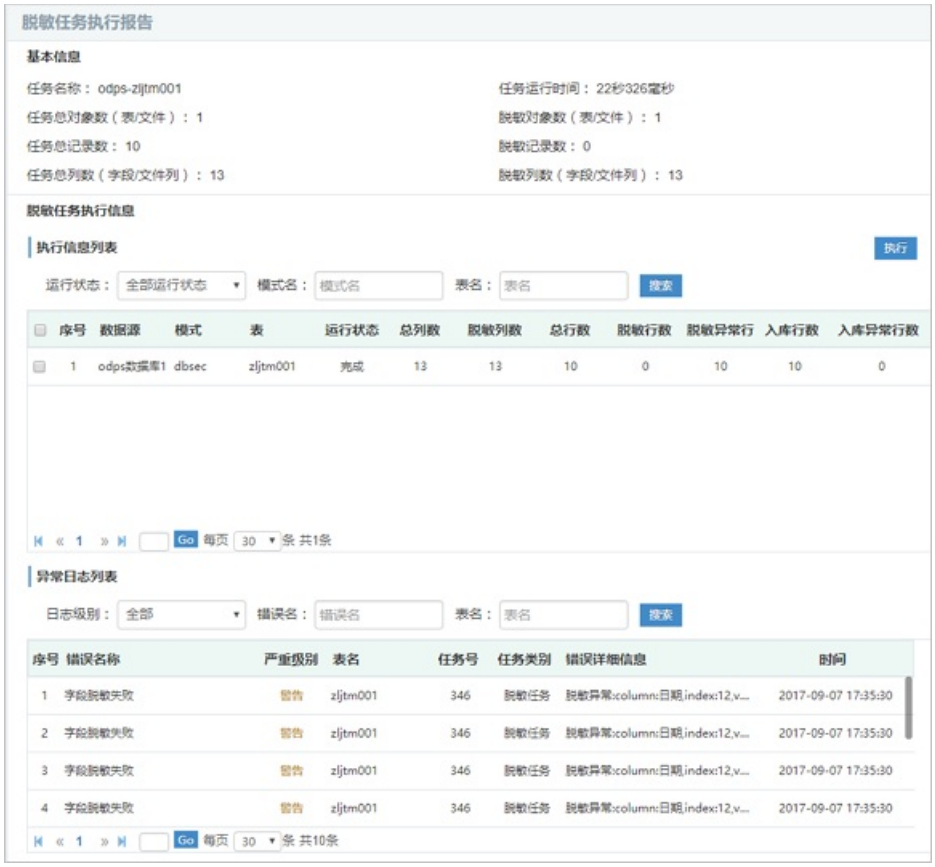
3. 在**脱敏任务执行记录**对话框中，选择已执行的任务记录，单击执行报告按钮，如脱敏任务执行记录所示。

脱敏任务执行记录



4. 在**脱敏任务执行报告**页面，查看该脱敏任务的执行报告，如脱敏任务执行报告所示。

脱敏任务执行报告



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。
2. 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**，如脱敏任务列表所示。

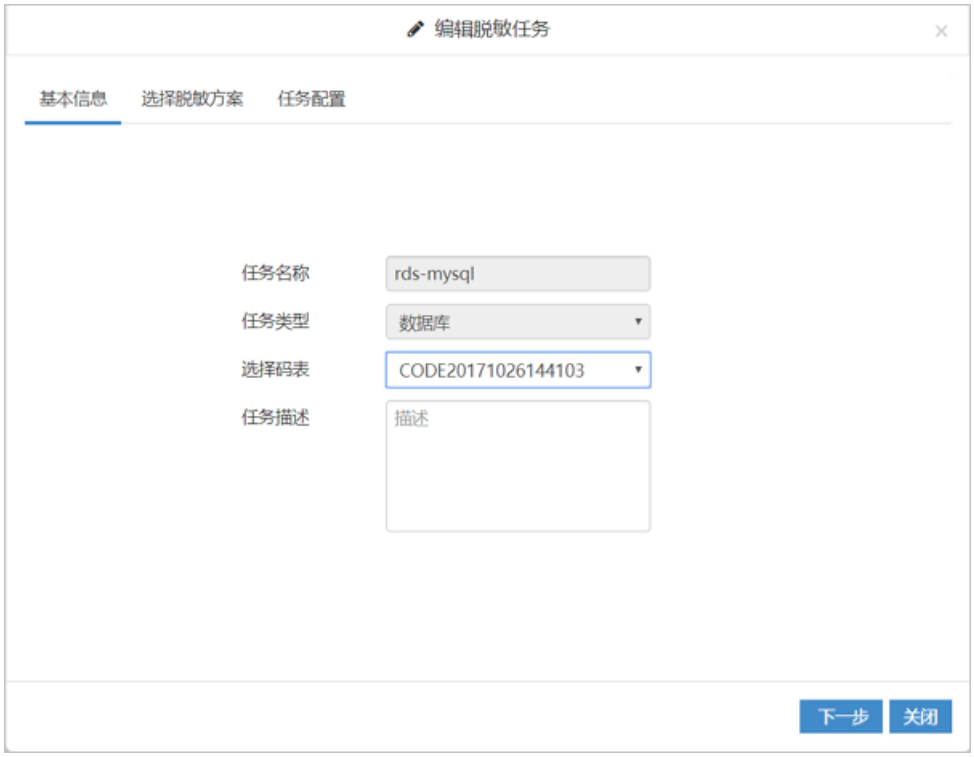
   脱敏任务列表



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**，如编辑脱敏任务所示。

   > **说明** 任务名称、任务类型无法修改。

   编辑脱敏任务



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。
2. 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**，如删除脱敏任务所示。

   删除脱敏任务



3. 在**信息提示**对话框中，单击**确定**，删除该脱敏任务。

10.6.2.3.4.2. 文件脱敏任务

添加文件脱敏任务

背景信息

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。

操作步骤

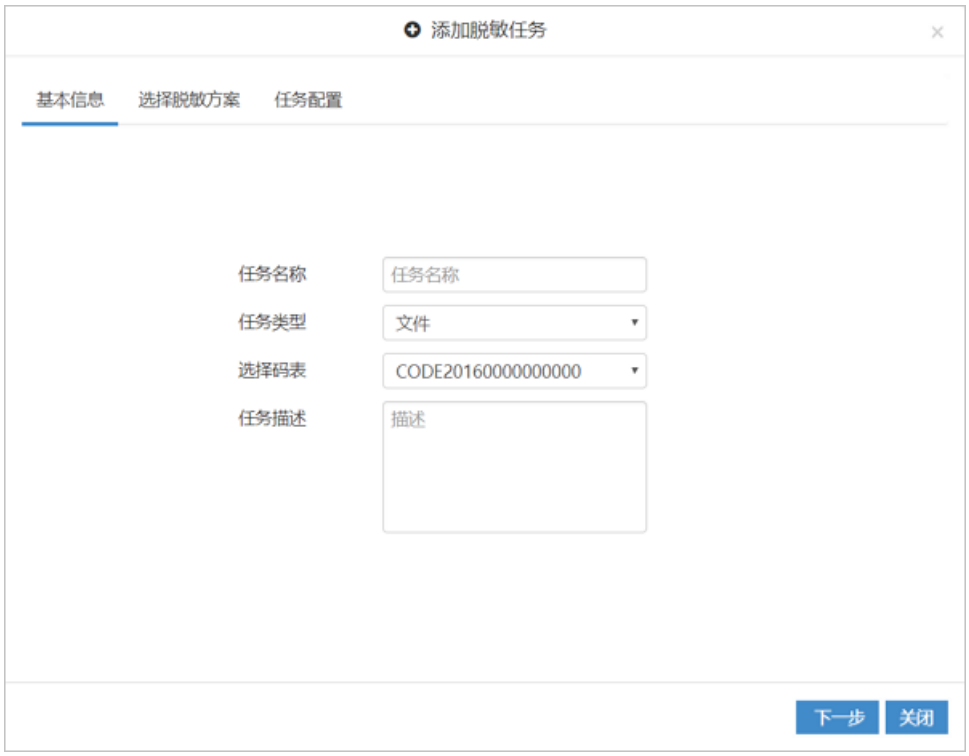
1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏 > 脱敏任务**页面，单击右上角的**添加**，如脱敏任务列表所示。

   脱敏任务列表



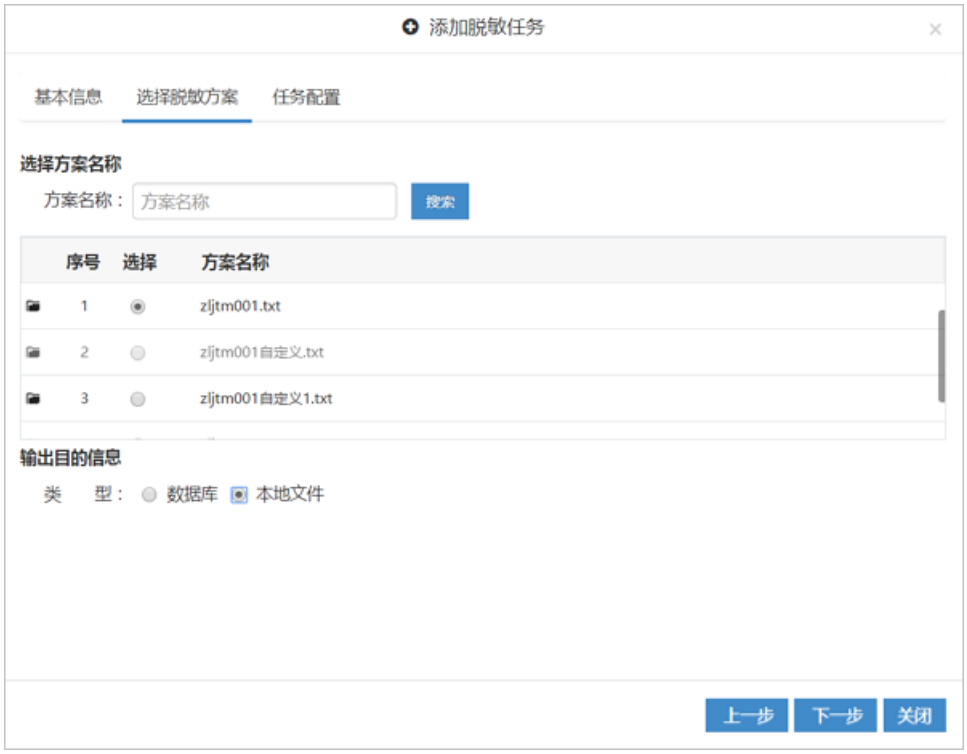
3. 在**添加脱敏任务**对话框的基本信息页签，输入任务名称、任务描述，选择任务类型为文件，选择码表，单击**下一步**，如添加脱敏任务基本信息所示。

   添加脱敏任务基本信息



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**，如选择脱敏方案所示。

   选择脱敏方案



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。

   添加脱敏任务任务配置



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。
2. 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**，如脱敏任务列表所示。

   脱敏任务列表



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**，如运行脱敏任务所示，执行该脱敏任务。

   运行脱敏任务



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。
2. 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**，如停止脱敏任务所示。

   停止脱敏任务



3. 在**信息提示**对话框中，单击**确定**。

查看文件脱敏任务的历史任务

操作步骤

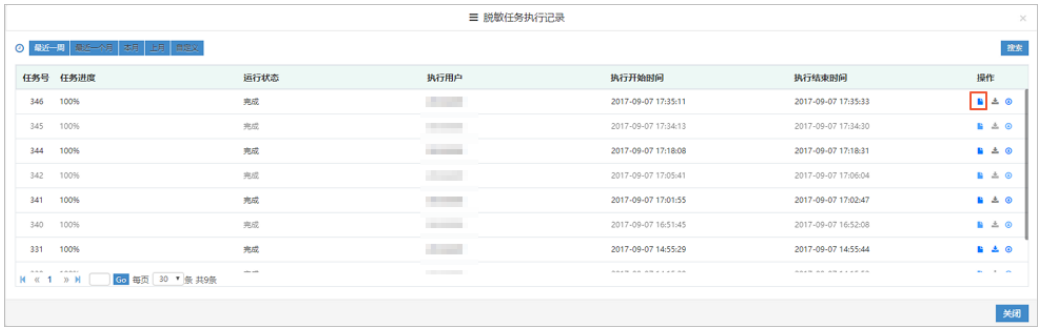
1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏 > 脱敏任务**页面，在**脱敏任务列表**中选择已完成的文件脱敏任务，单击任务记录右侧的操作列表，单击**历史任务**，如脱敏任务列表所示。

   脱敏任务列表



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，如脱敏任务执行记录所示。

   脱敏任务执行记录



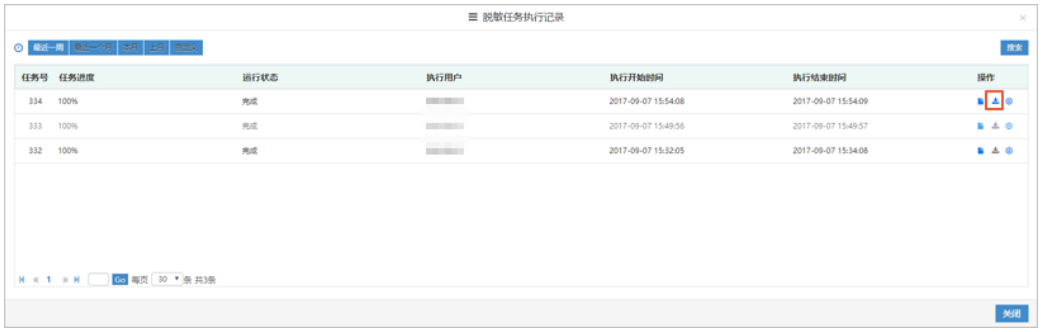
4. 在**脱敏任务执行报告**页面，查看该脱敏任务的执行报告，如脱敏任务执行报告所示。

   脱敏任务执行报告



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，如下载脱敏后的文件所示，可下载脱敏后的文件。

   下载脱敏后的文件



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。
2. 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**，如脱敏任务列表所示。

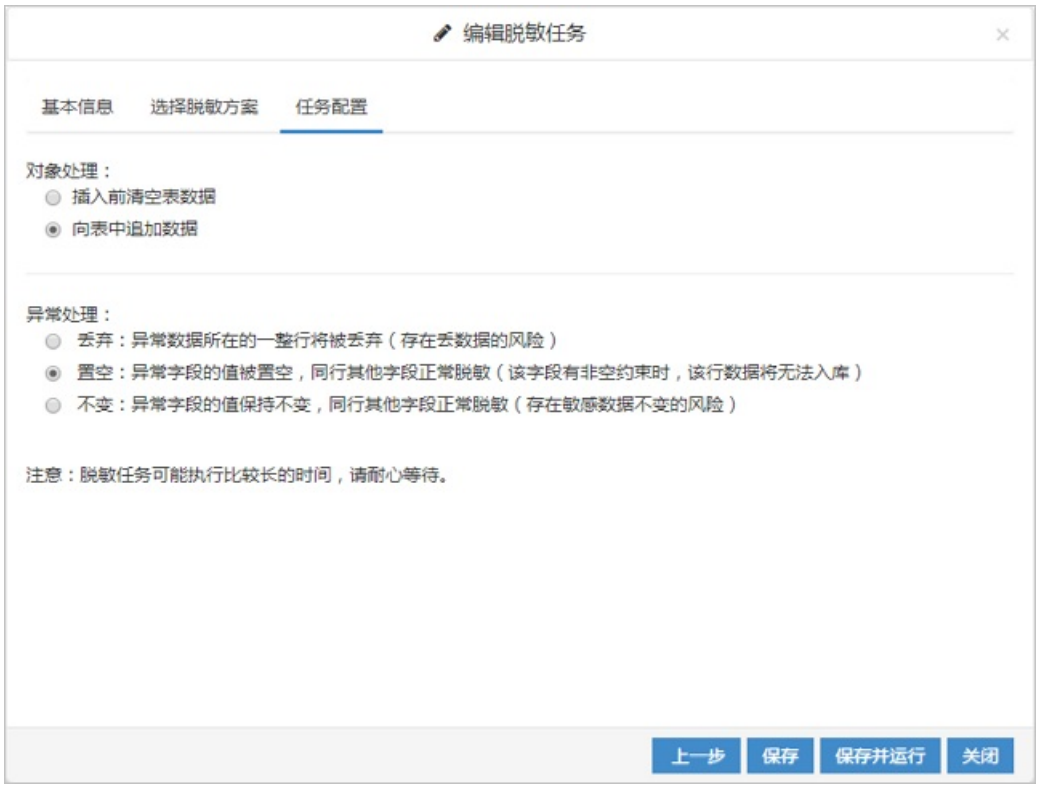
   脱敏任务列表



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**，如编辑脱敏任务所示。

> 说明 任务名称、任务类型无法修改。

编辑脱敏任务



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。
2. 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**，如删除脱敏任务所示。

删除脱敏任务



3. 在**信息提示**对话框中，单击**确定**，删除该脱敏任务。

10.6.2.3.4.3. 查询脱敏任务

操作步骤

1. 登录专有云数据安全控制台。
2. 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**，如搜索脱敏任务所示，查询符合相应条件的所有脱敏任务。

   搜索脱敏任务



10.6.2.3.5. 脱敏算法

10.6.2.3.5.1. 查看脱敏算法

背景信息

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。

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，如查看脱敏算法所示。

   查看脱敏算法



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。

10.6.2.3.5.2. 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**，如添加脱敏算法所示。

   添加脱敏算法



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**。

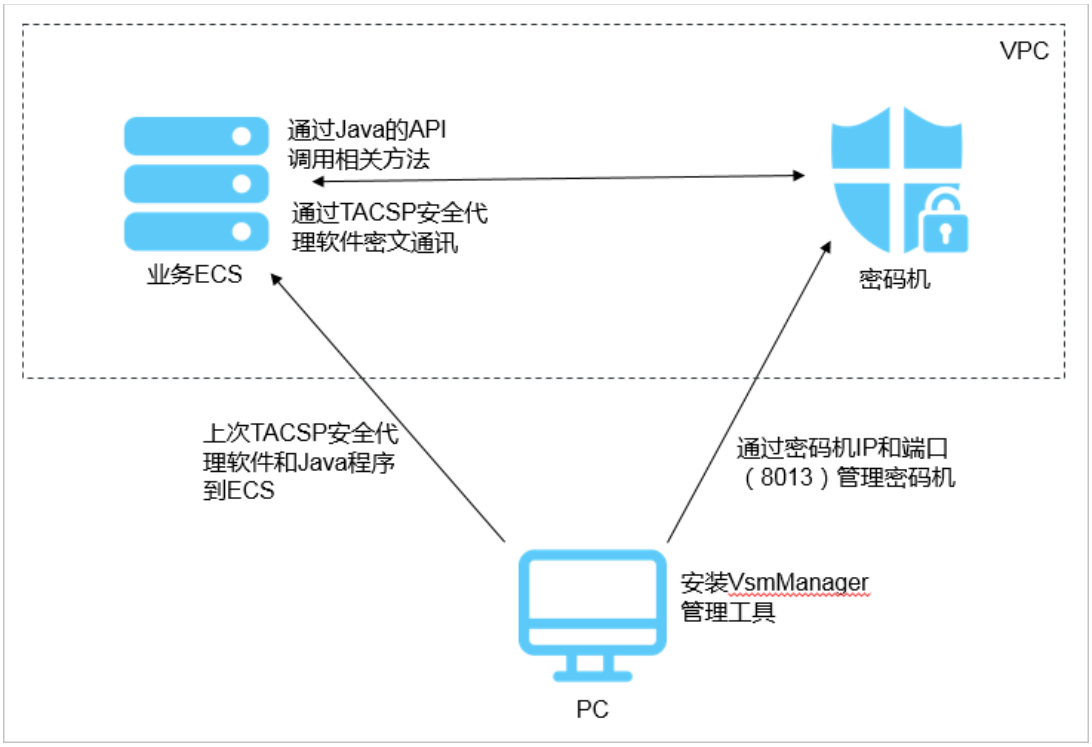
10.7. 加密服务

10.7.1. 概述

加密服务是一款云上加密解决方案。服务底层使用经国家密码管理局检测认证的硬件密码机，通过虚拟化技术，帮助您满足数据安全方面的监管合规要求，保护云上业务数据的隐私性要求。

借助加密服务，您能够对密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

加密服务的通信模式如下图所示，ECS和密码机需要都在VPC网络中。



功能介绍

加密服务提供以下功能：

- 密钥管理：密钥的安全存储和使用、分散产生子密钥、安全报文形式的导入导出。
- 数据加密：全面支持国产算法以及部分国际通用密码算法，满足您各种加密算法需求。
- 数据MAC计算：支持PBOC规范中定义的不同算法MAC运算。
- 交易认证：遵循PBOC2.0、3.0规范的ARQC验证和ARPC产生运算。

10.7.2. 快速入门

10.7.2.1. 使用流程

本文介绍了如何快速开始加密服务功能。

具体步骤如下：

1. 注册管理员UKEY

   登录之前，需要先注册管理员UKEY。管理员UKEY主要用途包括用户开机、协商通讯和管理工具与密码机通讯运算。

2. 登录VsmManager管理工具

   使用管理员UKEY登录VsmManager管理工具。

3. 执行原始初始化

   完成原始初始化，制作主密钥成份UKEY和授权UKEY，并合成设备主密钥（DMK）。

4. 授权操作

   需要授权后才能进行设备管理和主机服务。

5. 生成密钥

   在加密机中生成密钥，本章节以生成对称密钥为例。

6. 配置主机端口属性

   配置加密机的通讯方式，使用*密文通讯*提升安全性和可靠性。

7. 签发应用许可

   生成TACSP的应用许可证。

8. 配置TACSP

   在ECS上安装和配置TACSP。

9. 配置密文通讯

   配置加密机和ECS之间使用密文通讯。

10. 创建Demo实例

    在Eclipse上创建Demo实例，调用加密API。

10.7.2.2. 创建和配置加密实例

本文介绍了如何创建和配置加密实例。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**数据安全 > 加密服务**，单击**创建实例**。
3. 选择加密实例的**区域**、**虚拟网络**、**设备厂商**和**设备型号**等信息。
4. 单击**创建实例**，完成加密实例的创建。
5. 在新创建加密实例的**操作**栏，单击**配置**。
6. 在**配置IP**对话框中，配置VPC网络和IP地址。

配置项	说明
所属的VPC网络ID	选择VPC网络ID，加密服务需要和应用服务器属于同一个VPC。
所属的VPC子网	选择VPC子网网段。
分配私网IP地址	设置私网IP，该IP需要在**所属的VPC子网**的网段中。

7. 单击**确定**，完成加密实例的配置。

10.7.2.3. 注册管理员UKEY

本文介绍了如何注册管理员UKEY。

前提条件

PC能够访问密码机所在的VPC网络。

背景信息

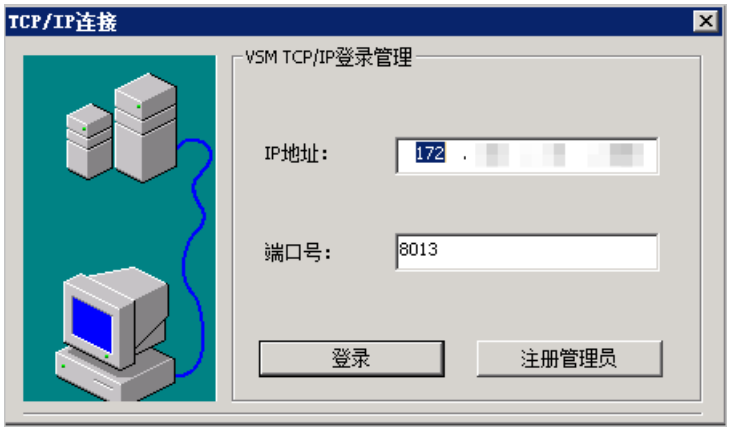
在登录VsmManager管理工具时，需要先注册管理员UKEY。

管理员UKEY用途包括：用户开机、协商通讯、管理工具与密码机通讯运算。

操作步骤

1. 在PC上双击*VsmManager.exe*管理工具。
2. 选择**系统 > VSM登录管理**。
3. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

   > **说明** 端口固定为8013。



4. 在PC上插入空UKEY，单击**注册管理员**。
5. 在**UKEY列表**窗口中选择插入的空UKEY，单击**确定**。



6. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

   > **说明** 出厂初始的UEKY口令为 `12345678` 。

   完成管理员UKEY的注册。

10.7.2.4. 登录VsmManager管理工具

本文介绍了如何登录VsmManager管理工具。

背景信息

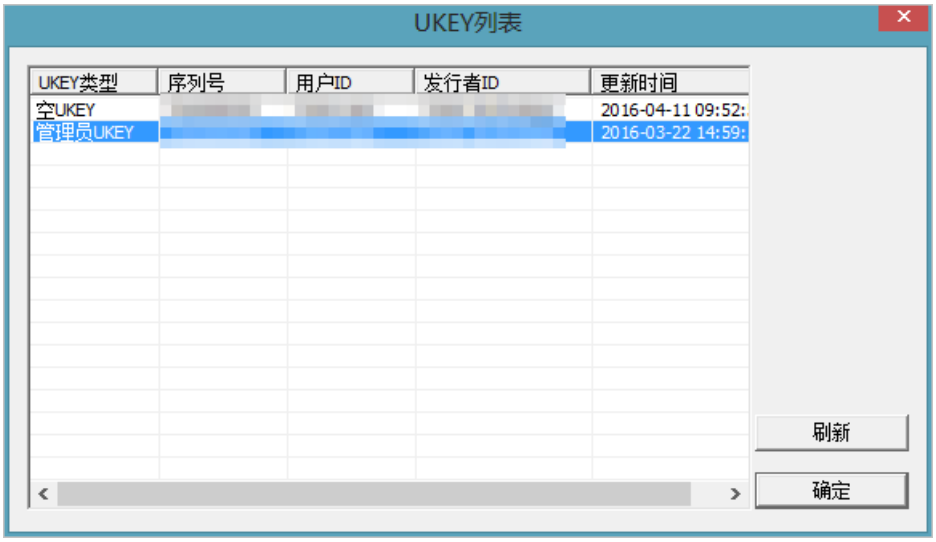
如果在没有注册UKEY管理员的情况下直接登录系统，您将不能进行原始初始化和恢复初始化操作，仅可以在测试主密钥的环境下进行密钥管理。

操作步骤

1. 在PC上插入管理员UKEY。
2. 双击*VsmManager.exe*管理工具。
3. 选择**系统 > VSM登录管理**。
4. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

   > **说明** 端口固定为8013。

5. 单击**登录**。
6. 在弹出的**UKEY列表**窗口中，选中**管理员UKEY**，单击**确定**。



7. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
8. 在登录成功确认框中，单击**确定**。

   登录成功后，进入VsmManager管理工具。

10.7.2.5. 执行原始初始化

该章节介绍如何进行原始初始化。

背景信息

密码机要投入生产环境时，必须先完成原始初始化操作，制作主密钥成份UKEY和授权UKEY，并合成设备主密钥（DMK）。

在进行原始初始化前，请规划好以下项目：

规划项目	说明	举例
设备主密钥（DMK）管理人员	需要几个DMK管理员持有主密钥成份UKEY。 取值范围：2~8	本章节以配置2个为例。
设备授权控制人员	需要几个设备授权控制人员持有授权UKEY。 取值范围：1、3、5	本章节以配置1个为例。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 原始初始化** 。

   注意 如果进行原始初始化操作，密码机将清除内部的全部密钥。

3. 在**安全操作警示**提示框中，单击**下一步**。
4. 在**请输入成份数目**中输入*2*，单击**下一步**。

   根据规划的设备主密钥（DMK）管理人员，确定主密钥成份UKEY数目，设置范围为2~8。本章节以2个为例。



5. 依次制作2个主密钥成份UKEY，单击**下一步**。



i. 第一个主密钥管理员两次输入预定义的秘密值，或者单击**随机秘密值**。
   - 手动设置秘密值为：8-32个任意字符。
   - 自动的随机秘密值为：32个任意字符。

ii. PC上插入空UKEY。

iii. 单击**产生成份UKEY**。

iv. 在弹出的**UKEY列表**中，选择刚才插入的空UKEY，单击**确定**。

v. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

   通过系统计算得到的成份数据写入UKEY中。

vi. 参考步骤~步骤，制作第二个主密钥成份UKEY。

6. 依次导入2个主密钥成份UKEY到系统，单击**下一步**。



i. 单击**导入成份**。

ii. 在**UKEY列表**中，第一个主密钥管理员选择自己的主密钥成份UKEY，单击**确定**。

系统将读取UKEY内的成份数据。

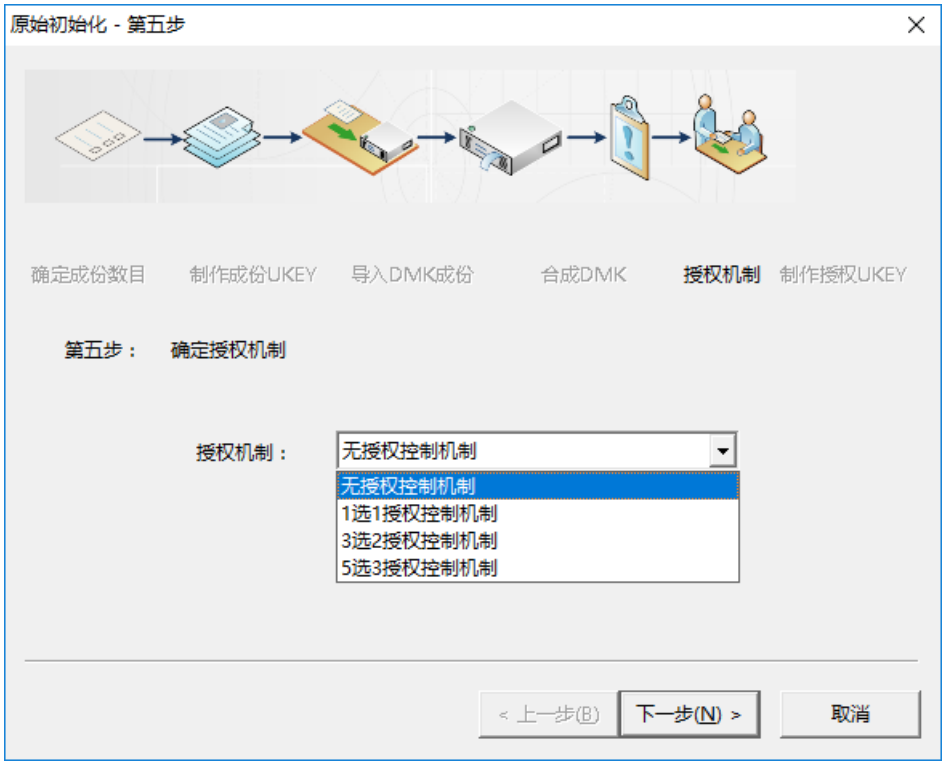
iii. 参考步骤~步骤，导入第二个主密钥成份UKEY。

> **说明** 主密钥成份UKEY的导入次序没有要求，但不能将同一个主密钥成份UKEY多次导入。

7. 单击**合成DMK**，完成后单击**下一步**。



8. **授权机制**选择*1选1授权控制机制*，单击**下一个**。



本章节以选择*1选1授权控制机制*为例，所有可选的授权机制如下：

授权机制	说明
无授权机制	不需要授权。

授权机制	说明
1选1授权控制机制	1个授权UEKY由1个授权人员保管，当为某类操作授权时，需1个授权人员授权许可。
3选2授权控制机制	m选n授权控制机制，制作m个授权UKEY由m个授权人员保管，当为某类操作授权时，需半数以上的授权人员授权许可，即n个授权UKEY认证通过。
5选3授权控制机制	

9. 制作授权UKEY。
   i. PC上插入空UKEY。
   ii. 单击**制作授权卡**。
   iii. 在**UKEY列表**中，选择插入的空UKEY，单击**确定**。
   iv. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
   v. （可选）参考步骤~步骤，依次制作余下授权UKEY。
   如果选择多个授权UKEY，需要根据提示依次制作授权UKEY。
10. 单击**完成**。
    完成原始初始化，密码机生成新的主密钥DMK。

10.7.2.6. 授权操作

本文介绍如何进行授权。

背景信息

部分设备管理操作和主机指令应用需要获取授权许可，密码机支持严格灵活的授权管理控制。授权具有以下优点：

- 授权机制可配置
  支持1选1、3选2、5选3和无授权控制机制。授权控制机制需在初始化的过程中设置，完成初始化后不允许被修改。
- UKEY授权机制
  通过验证授权UKEY完成对授权人员的身份识别，安全可靠。
- 分类分时授权控制
  通过授权UKEY验证后，可选择本次授权的操作类别及给予授权的时间，当某类操作授权的时效过期后，其授权许可将自动失效。

> **说明** 初始化时，如果**授权机制**配置为*无授权控制机制*，所有的操作均不受限。则本文不需要设置。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**设备管理 > 操作授权**。
3. 根据提示依次插入授权UKEY，输入口令，单击**下一步**。

系统将根据授权机制要求半数以上的授权UKEY验证通过。授权UKEY的验证次序无关，但重复验证无效。

4. 配置授权操作信息。

   可同时为多个类别授权不同的时限。



   授权类别说明

主类	子类	操作范围说明
设备管理	设备配置更新	重置端口属性，包括主机服务端口。
	应用密钥管理	○ 随机产生内部存储的密钥。 ○ 成份形式合成对称密钥。 ○ 删除内部对称或非对称密钥。 ○ 清除内部对称或非对称密钥。 ○ 内部密钥备份导出。
主机服务	账户PIN解密	使用BA、NG主机命令。
	产生公钥MAC	使用EO、TQ主机命令。
	内部密钥更新	○ KR、KD、KI、SI、TW、TY，内部存储模式的对称密钥的产生或导入。 ○ EI、EK、EJ、TS，内部存储模式的RSA密钥对的产生或导入。 ○ E0、E1、TU，内部存储模式的SM2密钥对的产生或导入。

5. 单击**完成**。

10.7.2.7. 生成密钥

本文介绍如何生成密钥。

前提条件

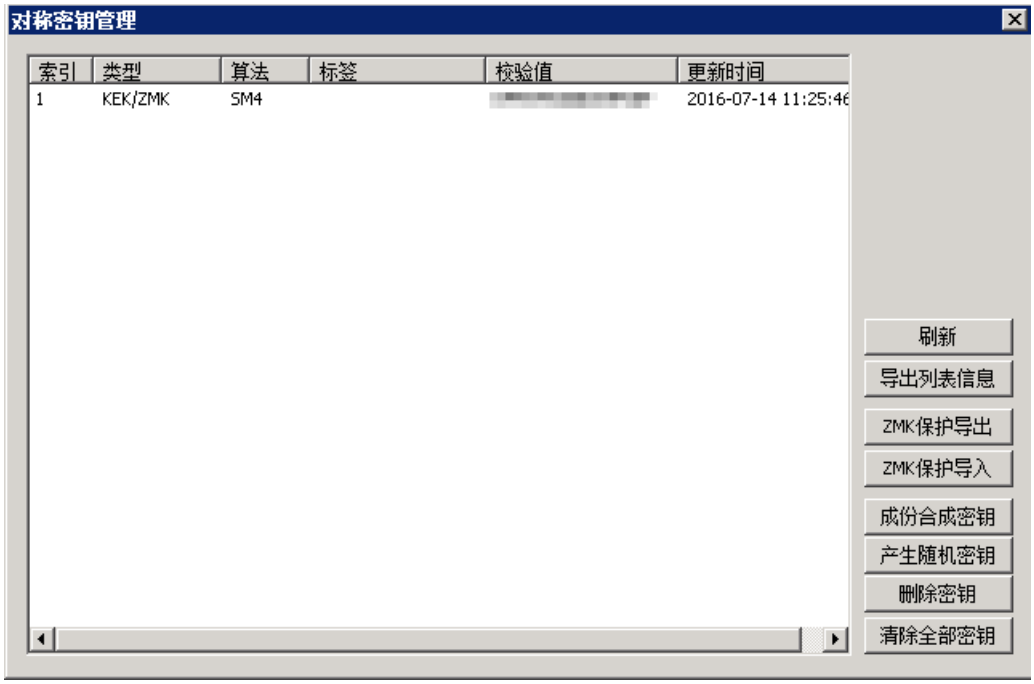
需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

背景信息

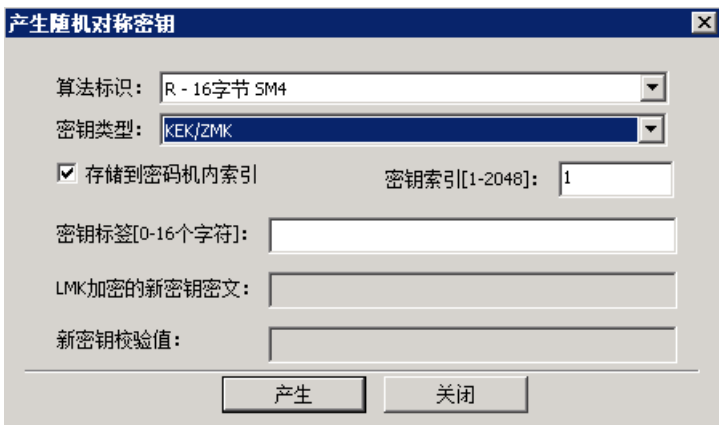
本文以生成对称加密密钥为例，如果想生成非对称密钥，请参见产生随机密钥。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 单击**产生随机密钥**。
4. 在对话框中配置对称密钥参数。



对称密钥参数

配置项	说明
算法标识	密码机支持多种对称密码算法，使用时根据其算法标识使用相应的密码算法。标识如下： ○ *Z*：单倍长的DES算法密钥。 ○ *U*：双倍长的3DES算法密钥，LMK加密输出时使用变量方式。 ○ *T*：三倍长的3DES算法密钥，LMK加密输出时使用变量方式。 ○ *X*：双倍长的3DES算法密钥。 ○ *Y*：三倍长的3DES算法密钥。 ○ *P*：SM1算法密钥。 ○ *R*：SM4算法密钥。 ○ *L*：AES-128算法密钥。 ○ *M*：AES-192算法密钥。 ○ *N*：AES-256算法密钥。
密钥类型	不同密钥类型具有不同的用途。
存储到密码机内索引	生成的密钥是否存储到密码机索引。
密钥索引	选中**存储到密码机内索引**后，设置索引号。 取值范围：1~2048
密钥标签	用于在密钥内部存储时标记密钥的标签说明。
LMK加密的新密钥密文	生成的密钥密文。
新密钥校验码	新密钥的校验码。

5. 单击**产生**。

   产生新的随机密钥并输出显示密文和校验值。

10.7.2.8. 配置主机端口属性

本文介绍如何配置主机端口属性。

背景信息

密码机和ECS之间的服务通讯方式出厂默认配置为明文通讯。

若要配置为密文通讯，则主机端口属性需要设置为*密文通讯*，同时还需要在TACSP安全代理软件进行相应的配置，以保证应用能够正常调用密码服务。密文通讯服务配置，参见配置密文通讯。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**设备管理 > 主机服务端口属性**。
3. 设置主机端口属性。

> **说明** 需要根据实际需求正确配置主机端口属性。



主机端口属性

属性	说明
Socket KeepAlive时间	TCP连接保活探测时间，单位：秒。 取值范围：60~600
消息报文头长度	主机报文消息头长度，单位：字节。 取值范围：60~600
消息报文编码格式	主机报文的编码格式。 ○ ASCII ○ EBCDIC
主机服务通讯方式	○ 明文通讯：与主机服务间的通讯为明文。 ○ 密文通讯：与主机服务间的通讯为密文。

10.7.2.9. 签发应用许可

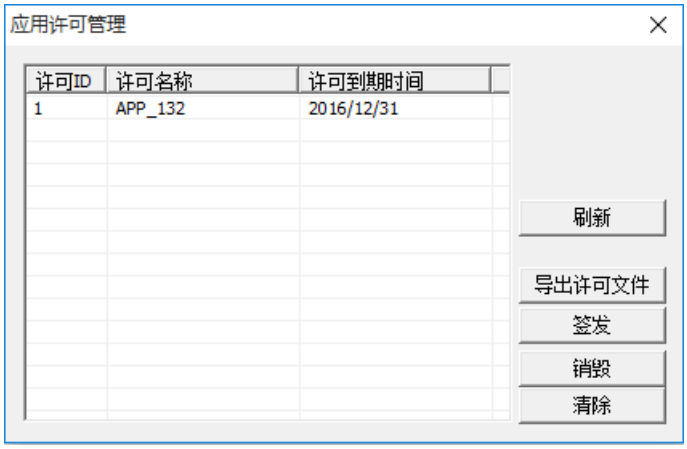
本文介绍如何签发应用许可。

背景信息

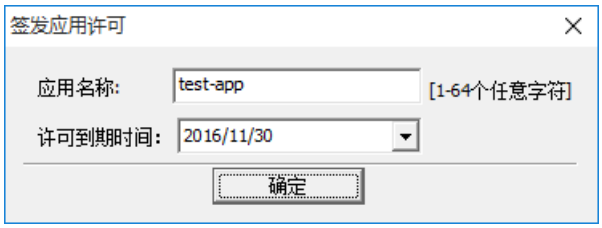
配置密文通讯时，需要为TACSP签发应用许可。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**设备管理 > 应用许可管理**。
3. 单击**签发**。



4. 设置应用名称和到期时间。



5. 单击**确定**。

   生成应用许可文件（*.license*后缀的文件），并自动导出到VsmManager管理工具所在目录。

10.7.2.10. 配置TACSP

本文介绍如何配置TACSP安全代理软件。TACSP安全代理软件基于密码机的安全应用而设计开发的安全代理软件，是集多机热备、负载均衡功能为一体的密码机应用平台。

前提条件

ECS和密码机在同一个VPC网络中。

背景信息

TACSP安全代理软件支持的操作系统和加密方式如下。

- 操作系统：支持Linux、AIX、HP-UNIX等类UNIX操作系统。
- 加密方式：支持以Socket方式提供密码安全服务，应用程序通过Socket方式访问安全代理软件。

操作步骤

1. 通过FTP软件上传TACSP安全代理软件到业务ECS。
2. 通过SSH登录业务ECS。
3. 进入TACSP所在路径。
4. 配置*tacsp_cfg.ini*。

   *tacsp_cfg.in*配置文件内容如下：

```
[TACSP_IPC]
COMMAND_QUEUE_KEY               = 130
RESPONSE_QUEUE_KEY              = 131
SHARED_MEMORY_KEY               = 132
LOG_LEVEL                       = 1
[TACSP_SERVERINFO]
LISTEN_IP_FLG                   = 0
LISTEN_PORT                     = 9999
HSM_LOADSIZE                    = 2
HSM_LOADSELF                    = 0
[TACSP_HSMINFO]
HSM_COUNT                       = 0
TOTAL_TIMEOUT                   = 6
SINGLEHSM_TIMEOUT               = 2
[TACSP_HSM00]
HSM_TYPE                        = SJJ1310
HSM_IP                          = 192.*.*.51
HSM_PORT                        = 8018
HSM_WEIGHT                      = 10
HSM_ENC_COMM                    = 0
[TACSP_HSM01]
HSM_TYPE                        = SJJ1310
HSM_IP                          = 192.*.*.102
HSM_PORT                        = 8018
HSM_WEIGHT                      = 10
HSM_ENC_COMM                    = 1
```

配置说明

节点	键名	说明
TACSP_IPC	无	TACSP使用的IPC相关ID。
	COMMAND_QUEUE_KEY	TACSP使用2个队列和1个共享内存。 此处配置的队列ID和共享内存ID，必须确保与当前系统中的相关ID不冲突。 取值范围：1~65537
	RESPONSE_QUEUE_KEY	
	SHARED_MEMORY_KEY	
	LOG_LEVEL	日志级别： ○ *0*：不记录任务日志。 ○ *1*：记录错误日志。 ○ *2*：记录连接信息。 ○ *3*：记录调试信息日志。
	无	对外提供Socket服务配置信息。

节点	键名	说明
TACSP_SERVERINFO	LISTEN_IP_FLG	○ *0*：默认值，监听127.0.0.1 ○ *1*：监听0.0.0.0
	LISTEN_PORT	负载热备对外提供的监听端口。 取值范围：1025~65535
	HSM_LOADSIZE	头部中表示报文长度的字节数。
	HSM_LOADSELF	头部表示报文长度中是否包含自身长度： ○ *0*：不包含 ○ *1*：包含
TACSP_HSMINFO	无	密码机相关信息。
	HSM_COUNT	密码机数量。 取值范围：1~20
	TOTAL_TIMEOUT	每次Socket通讯总的超时时间，单位：秒。 建议取值：加密机个数 * 单台加密机通讯超时 + 2
	SINGLEHSM_TIMEOUT	每台加密机每次Socket通讯的超时时间，单位：秒。
TACSP_HSM*xx*	无	某索引密码机的信息，有n个密码机，必须有n个节配置。 *xx*取值范围：00~（n-1）
	HSM_TYPE	密码机类型
	HSM_IP	密码机的IP地址
	HSM_PORT	密码机的端口号
	HSM_WEIGHT	密码机的工作权重，即安全代理软件和此台加密机有多少个Socket连接。 取值范围：1~65
	HSM_ENC_COMM	和密码机的通讯模式： ○ *0*：明文通讯 ○ *1*：密文通讯

5. （可选）配置环境变量TACSPCFG和CLUSTERDEBUG环境变量。

> **说明** 如不配置TACSPCFG，则配置文件必须在TACSP安全代理软件所在的路径下；如不配置CLUSTERDEBUG，则日志将默认输出在TACSP安全代理软件所在的路径下。

i. 编辑*/etc/profile*。

```
vi /etc/profile
```

ii. 在*/etc/profile*中添加变量。

```
export TACSPCFG=tacsp_cfg.ini所在目录
export CLUSTERDEBUG=日志存储目录
```

iii. 使环境变量立即生效。

```
source /etc/profile
```

10.7.2.11. 配置密文通讯

本文介绍如何配置密文通讯。

背景信息

密文通讯方式是指应用主机与密码机之间的通讯采用加密的方式，能够在专有云的环境下提供更安全更可靠的加密服务。

操作步骤

1. 配置主机端口属性。

   主机服务通讯方式修改为*密文通讯*。

2. 签发应用许可证。

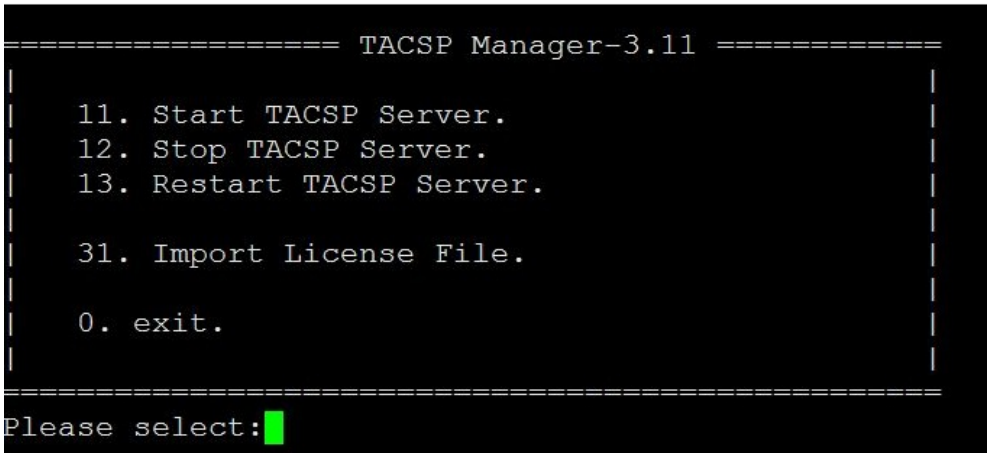
   应用许可的内容包括VSM设备公钥、TACSP公私钥、应用名称、签发时间、到期时间及设备私钥对前述内容的签名。

   > **说明** 如果有多个密码机，分别导出应用许可证。

3. 应用许可证通过FTP上传到TACSP安全代理软件所在路径。
4. 导入应用许可证。

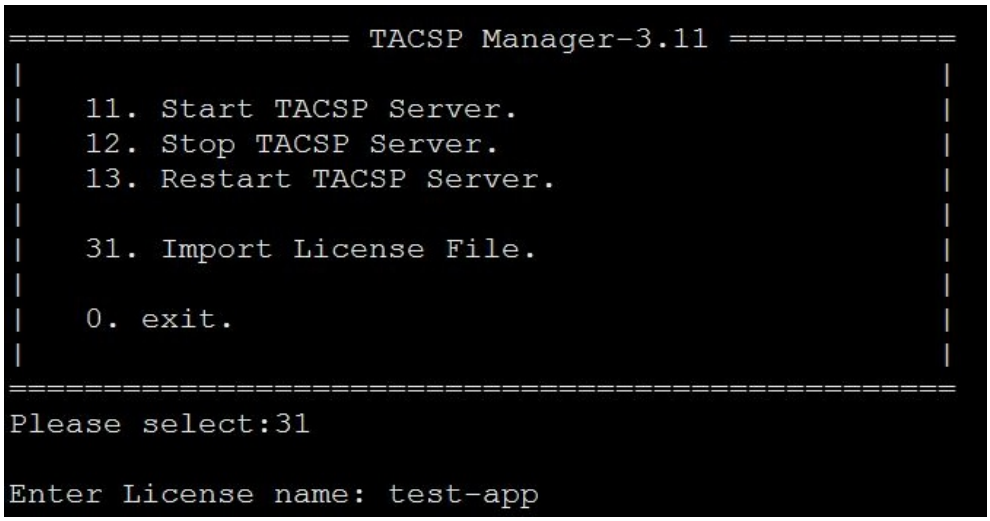
   i. SSH登录ECS并进入TACSP安全代理软件所在路径。

ii. 执行./keyMng。



iii. 输入*31*，按回车键（Enter）。

开始导入应用许可证。



iv. 输入许可证名称，按回车键（Enter）。

v. （可选）重复步骤4的c~d步骤，导入其他加密机的应用许可证。

如果有多台密码机，则需要依次导入其他密码机的应用许可证。

vi. 输入*11*，启动TACSP安全代理软件。

如果TACSP已经启动，则输入*13*，重启TACSP。

10.7.2.12. 创建Demo实例

本文介绍如何创建Java的Demo实例。

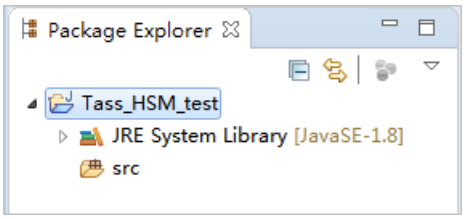
背景信息

VsmManager管理工具和密文通讯方式配置完成后，您就可以通过调用API接口，使用加密服务。

本文创建JAVA的Demo实例后，您可以通过JAVA源文件了解如何调用加解密的API接口，实例说明参见Demo实例说明。

操作步骤

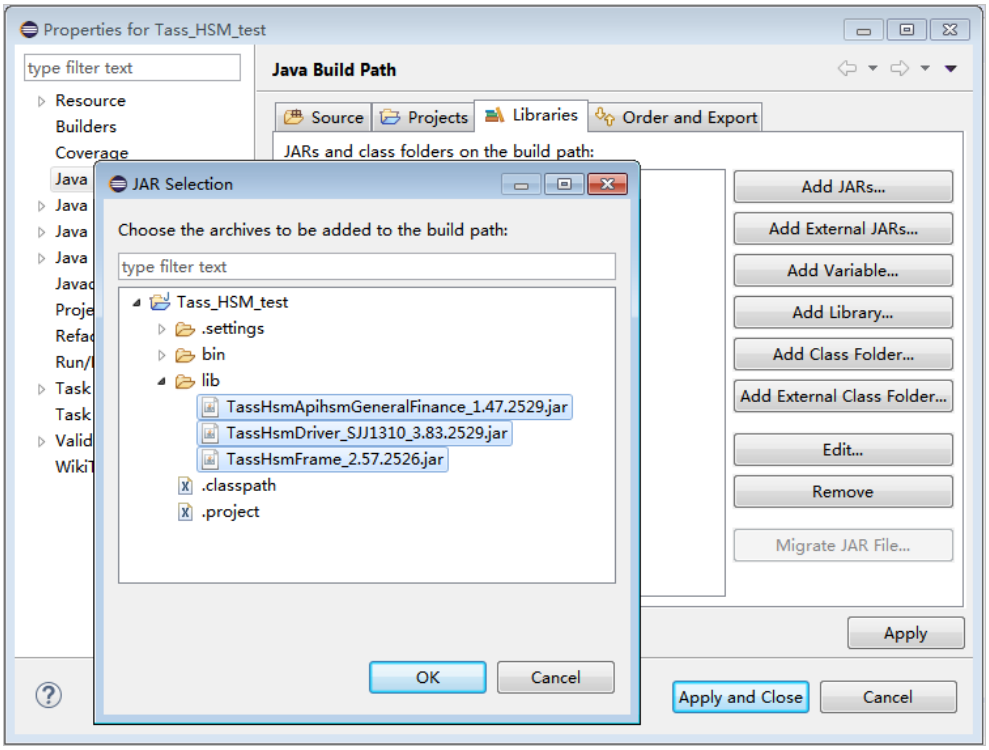
1. 在Eclipse中新建Java工程。
   i. 选择**File > New > Java Project**。
   ii. 在**Project name**中输入工程名称。
   iii. 单击**Finish**。
   创建Java工程实例如下所示。



2. 导入jar包。
   加密服务需要的3个jar包：
   - *TassHsmApihsmGeneralFinance_1.47.2529.jar*
   - *TassHsmDriver_SJJ1310_3.83.2529.jar*
   - *TassHsmFrame_2.57.2526.jar*

   i. 右键单击工程名称，选择**New > Folder**。
   ii. 在**Folder name**中输入*lib*，单击**Finish**。
   iii. 复制*TassHsmApihsmGeneralFinance_1.47.2529.jar*、*TassHsmDriver_SJJ1310_3.83.2529.jar*、*TassHsmFrame_2.57.2526.jar*包。
   iv. 右键单击**lib**，选择**Paste**。
   v. 右键单击工程名称，选择**Build Path > Configure Build Path**。

vi. 在Libraries页签下，单击Add JARs。



vii. 选择*lib*中的3个jar包，单击OK。

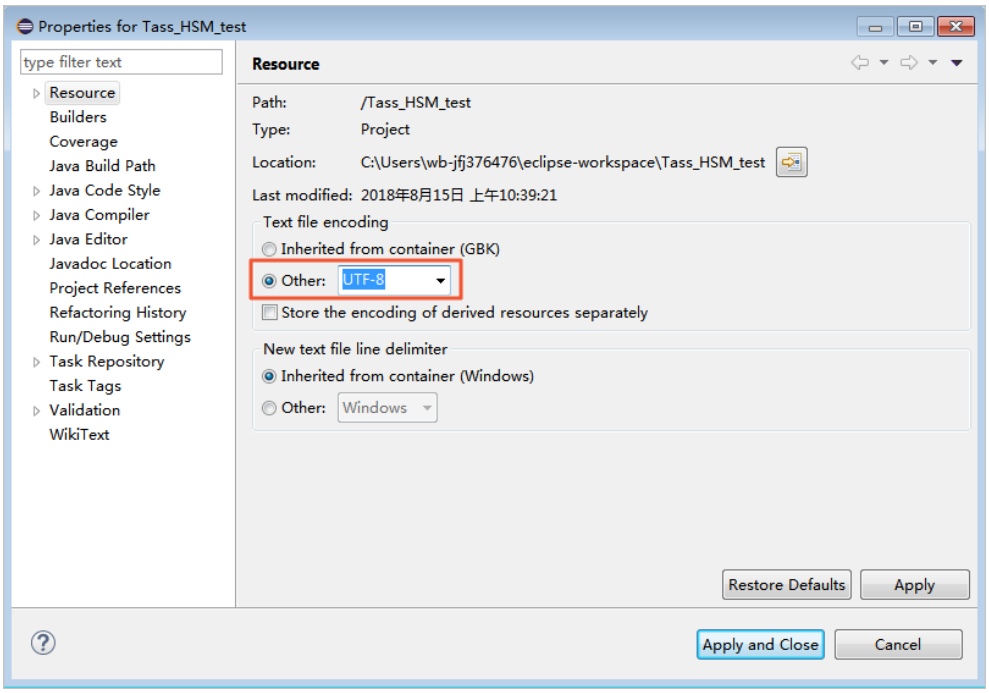
viii. 单击Apply and Close。

3. 修改编码格式为*UTF-8*。

i. 右键单击工程名称，选择Properties。

ii. 单击Resource。

iii. 在Text file encoding中选择Other，并在下拉菜单中选择*UTF-8*。



iv. 单击Apply and Close。

4. 复制Java实例文件到工程中。

Java demo文件：*test_hsmGeneralFinance.java*。

i. 复制*test_hsmGeneralFinance.java*。

ii. 右键单击*src*目录，选择Paste。

10.7.3. 加密实例管理

10.7.3.1. 创建加密实例

本文介绍了如何创建加密实例。

背景信息

在使用加密服务功能前，需要创建加密实例。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**数据安全 > 加密服务**。
3. 在**加密服务**界面，单击**创建实例**。
4. 选择加密实例的**区域**、**虚拟网络**、**设备厂商**和**设备型号**等信息。
5. 单击**创建实例**，完成加密实例的创建。

10.7.3.2. 配置加密实例

本文介绍了如何配置加密实例。

背景信息

加密服务实例需要配合专有网络（VPC网络）一起使用。即创建加密服务实例后，还需要再配置VPC网络和私有IP地址，才能正常使用。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中**数据安全 > 加密服务**。
3. 在新创建加密实例的**操作**栏，单击**配置**。
4. 在**配置IP**对话框中，配置VPC网络和IP地址。

配置项	说明
所属的VPC网络ID	选择VPC网络，加密服务需要和应用服务器属于同一个VPC。
所属的VPC子网	选择VPC子网网段。
分配私网IP地址	设置私网IP，该IP需要在**所属的VPC子网**的网段中。

5. 单击**确定**，完成加密实例的配置。

10.7.3.3. 释放加密实例

本文介绍了如何释放加密实例。

背景信息

加密实例资源是有限的，如果您不再需要加密服务后，可以通过释放操作，释放加密实例资源。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中选择**数据安全 > 加密服务**页面。
3. 在**加密服务**界面，找到需要释放的加密实例，在**操作**栏，单击**释放**。
4. 在提示对话框中，单击**确定**，释放加密实例。

10.7.4. 密码机管理

该章节介绍通过VsmManager管理工具管理密码机。

加密服务是云上的加密解决方案，为业务系统提供安全的应用层密码服务，保证业务数据产生、传输、接收到处理整个过程的安全性、有效性、完整性、不可抵赖性。

VsmManager管理工具是密码机管理工具，通过VsmManager管理工具可以实现以下管理操作：

- 系统管理：登录VsmManager管理工具。
- 密钥管理：包括设备主密钥管理和应用密钥管理。
- 设备管理：包括设备配置、授权管理和UKEY管理。
- 设备诊断维护：包括日志管理、设备运行状态、系统维护。

10.7.4.1. 系统管理

10.7.4.1.1. 注册管理员UKEY

本文介绍了如何注册管理员UKEY。

前提条件

PC能够访问密码机所在的VPC网络。

背景信息

在登录VsmManager管理工具时，需要先注册管理员UKEY。

管理员UKEY用途包括：用户开机、协商通讯、管理工具与密码机通讯运算。

操作步骤

1. 在PC上双击*VsmManager.exe*管理工具。
2. 选择**系统 > VSM登录管理**。
3. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

> **说明** 端口固定为8013。



4. 在PC上插入空UKEY，单击**注册管理员**。
5. 在**UKEY列表**窗口中选择插入的空UKEY，单击**确定**。



6. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

> **说明** 出厂初始的UEKY口令为 `12345678` 。

完成管理员UKEY的注册。

10.7.4.1.2. 登录VsmManager管理工具

本文介绍了如何登录VsmManager管理工具。

背景信息

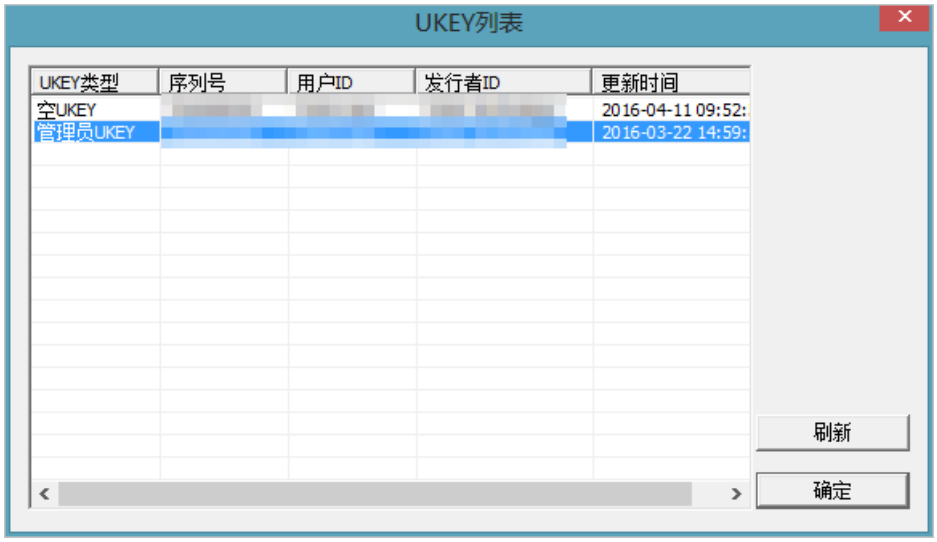
如果在没有注册UKEY管理员的情况下直接登录系统，您将不能进行原始初始化和恢复初始化操作，仅可以在测试主密钥的环境下进行密钥管理。

操作步骤

1. 在PC上插入管理员UKEY。
2. 双击*VsmManager.exe*管理工具。
3. 选择**系统 > VSM登录管理**。
4. 在**TCP/IP连接**对话框中，输入密码机的IP和端口号。

   > **说明** 端口固定为8013。

5. 单击**登录**。
6. 在弹出的**UKEY列表**窗口中，选中**管理员UKEY**，单击**确定**。



7. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
8. 在登录成功确认框中，单击**确定**。

   登录成功后，进入VsmManager管理工具。

10.7.4.2. 密钥管理

10.7.4.2.1. 执行原始初始化

该章节介绍如何进行原始初始化。

背景信息

密码机要投入生产环境时，必须先完成原始初始化操作，制作主密钥成份UKEY和授权UKEY，并合成设备主密钥（DMK）。

在进行原始初始化前，请规划好以下项目：

规划项目	说明	举例
设备主密钥（DMK）管理人员	需要几个DMK管理员持有主密钥成份UKEY。 取值范围：2~8	本章节以配置2个为例。

规划项目	说明	举例
设备授权控制人员	需要几个设备授权控制人员持有授权UKEY。 取值范围：1、3、5	本章节以配置1个为例。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 原始初始化** 。

   注意 如果进行原始初始化操作，密码机将清除内部的全部密钥。

3. 在**安全操作警示**提示框中，单击**下一步**。
4. 在**请输入成份数目**中输入*2*，单击**下一步**。

   根据规划的设备主密钥（DMK）管理人员，确定主密钥成份UKEY数目，设置范围为2~8。本章节以2个为例。



5. 依次制作2个主密钥成份UKEY，单击**下一步**。



i. 第一个主密钥管理员两次输入预定义的秘密值，或者单击**随机秘密值**。
   - 手动设置秘密值为：8-32个任意字符。
   - 自动的随机秘密值为：32个任意字符。

ii. PC上插入空UKEY。

iii. 单击**产生成份UKEY**。

iv. 在弹出的**UKEY列表**中，选择刚才插入的空UKEY，单击**确定**。

v. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。

   通过系统计算得到的成份数据写入UKEY中。

vi. 参考步骤~步骤，制作第二个主密钥成份UKEY。

6. 依次导入2个主密钥成份UKEY到系统，单击**下一步**。



i. 单击**导入成份**。

ii. 在**UKEY列表**中，第一个主密钥管理员选择自己的主密钥成份UKEY，单击**确定**。

系统将读取UKEY内的成份数据。

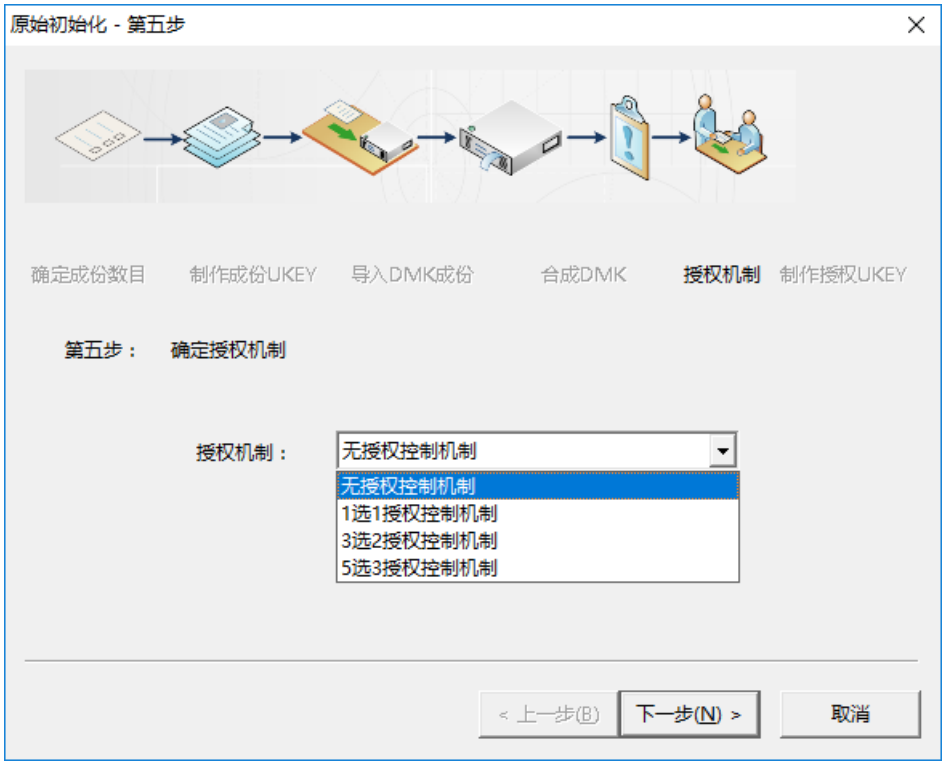
iii. 参考步骤~步骤，导入第二个主密钥成份UKEY。

> **说明** 主密钥成份UKEY的导入次序没有要求，但不能将同一个主密钥成份UKEY多次导入。

7. 单击**合成DMK**，完成后单击**下一步**。



8. **授权机制**选择*1选1授权控制机制*，单击**下一个**。



本章节以选择*1选1授权控制机制*为例，所有可选的授权机制如下：

授权机制	说明
无授权机制	不需要授权。

授权机制	说明
1选1授权控制机制	1个授权UEKY由1个授权人员保管，当为某类操作授权时，需1个授权人员授权许可。
3选2授权控制机制	m选n授权控制机制，制作m个授权UKEY由m个授权人员保管，当为某类操作授权时，需半数以上的授权人员授权许可，即n个授权UKEY认证通过。
5选3授权控制机制	

9. 制作授权UKEY。
   i. PC上插入空UKEY。
   ii. 单击**制作授权卡**。
   iii. 在**UKEY列表**中，选择插入的空UKEY，单击**确定**。
   iv. 在**VERIFY**对话框中，输入UKEY口令，单击**确定**。
   v. （可选）参考步骤~步骤，依次制作余下授权UKEY。
   如果选择多个授权UKEY，需要根据提示依次制作授权UKEY。
10. 单击**完成**。
    完成原始初始化，密码机生成新的主密钥DMK。

10.7.4.2.2. 执行恢复初始化

该章节介绍如何进行恢复初始化。

背景信息

通过恢复初始化操作，您可以使用主密钥成份UKEY恢复原来的DMK。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 恢复初始化** 。

   注意 如果进行恢复初始化操作，将清除密码机内所有的全部密钥。

3. 在**安全操作警示**提示框中，单击**下一步**。
4. 输入主密钥成份UEKY数目，单击**下一步**。
5. 依次导入主密钥成份UKEY，单击**下一步**。
   i. 单击**导入成份UKEY**。
   ii. 主密钥管理员选择自己的主密钥成份UKEY，并输入口令。
   系统将读取UKEY内的成份数据。
   iii. 参考步骤~步骤，依次导入主密钥成份UKEY。
   主密钥成份UKEY的导入次序没有要求，但不能将同一个主密钥成份UKEY多次导入。
6. 单击**合成DMK**，完成后单击**下一步**。
7. 确定授权机制。



- 如果多机备份的密码机共用一套授权UKEY，则选择**同步授权信息**。
  a. 选择**同步授权信息**。
  b. 单击**下一步**。
  c. 插入有效的授权UKEY，输入UKEY口令，单击**完成**。
  d. 单击**同步开始**。
- 如果每台密码机使用独立的授权UKEY，则选择**制作新的授权UEKY**。
  a. 选择**制作新的授权UEKY**。
  b. 在**选择授权机制**下拉菜单中，选择授权机制。
  c. 单击**下一步**。
  d. PC上插入第一个授权UKEY，输入UKEY口令。
  e. 单击**制作授权卡**。
  f. 参考上述两个步骤，依次制作余下授权UKEY。

10.7.4.2.3. 执行出厂初始化

该章节介绍如何进行出厂初始化。

背景信息

用户在进行系统开发或调试时，可以为密码机进行出厂初始化，内部自动装载测试主密钥，密码机内使用公开通用的本地主密钥（LMKs）。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 出厂初始化** 。

> 注意 如果进行原始初始化操作，将清除密码机内所有的全部密钥。

3. 在**安全操作警示**提示框中，单击**下一步**。
4. 在导入测试DMK步骤中，单击**下一步**。
5. 选择**授权机制**，单击**下一个**。

授权机制	说明
无授权机制	不需要授权。
1选1授权控制机制	1个授权UEKY由1个授权人员保管，当为某类操作授权时，需1个授权人员授权许可。
3选2授权控制机制	m选n授权控制机制，制作m个授权UKEY由m个授权人员保管，当为某类操作授权时，需半数以上的授权人员授权许可，即n个授权UKEY认证通过。
5选3授权控制机制	

6. 依次制作授权UKEY。
   i. PC上插入第一个授权UKEY，输入UKEY口令。
   ii. 单击**制作授权卡**。
   iii. 参考步骤~步骤，依次制作余下授权UKEY。

10.7.4.2.4. 获取DMK校验值

该章节介绍如何获取设备主密钥（DMK）校验值。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 获取DMK校验值** 。
   界面显示当前DMK校验值。

10.7.4.2.5. 备份DMK

该章节介绍如何备份DMK。

背景信息

DMK导出到多个成份UKEY中，当原有的主密钥成份UKEY丢失或损坏时，保证能够重新合成出原来的DMK。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 导出DMK成份** 。
3. 输入需要导出的成份UKEY数目，单击**下一步**。
   成份UKEY数目可设置范围为2~8。
4. 依次导出写入到成份UKEY。

10.7.4.2.6. 对称密钥管理

10.7.4.2.6.1. 产生随机密钥

本文介绍了如何产生随机密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

背景信息

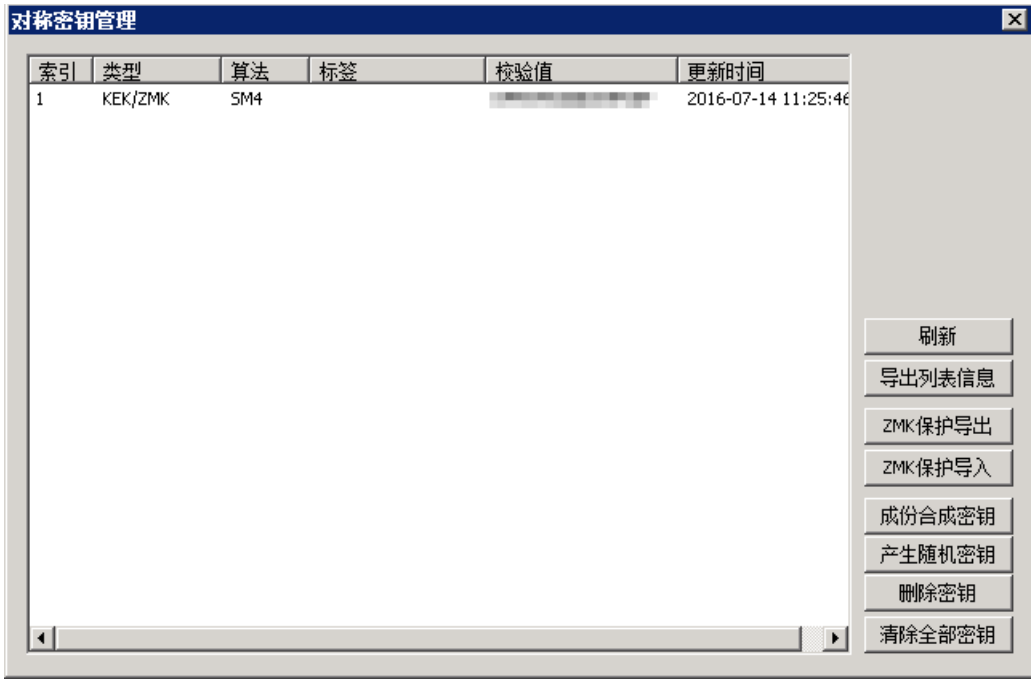
对称密钥状态信息如下表所示。

对称密钥状态信息

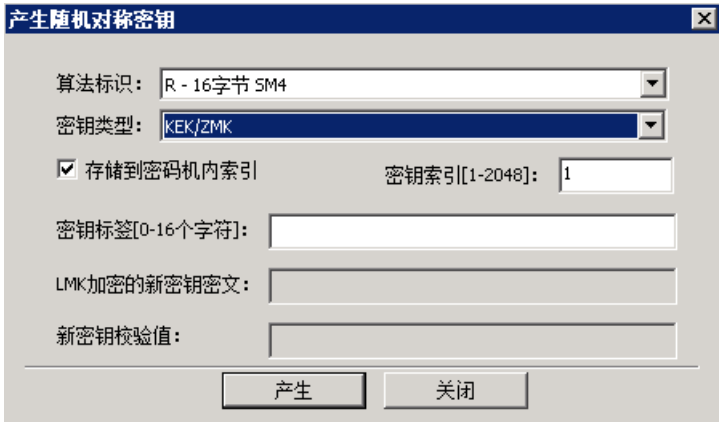
信息	说明
密钥索引号	对称密钥索引号范围：1~2048
密钥类型	密钥的类型
密钥算法	SM1、SM4、DES、DES2、DES3、AES
密钥标签	用户自定义的密钥标识，0~16个字符
校验值	密钥加密一个分组全0数据的密文，取前8字节
更新时间	密钥产生或导入的时间

操作步骤

1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 单击**产生随机密钥**。
4. 在对话框中配置对称密钥参数。



对称密钥参数

配置项	说明

配置项	说明
算法标识	密码机支持多种对称密码算法，使用时根据其算法标识使用相应的密码算法。标识如下： ○ *Z*：单倍长的DES算法密钥。 ○ *U*：双倍长的3DES算法密钥，LMK加密输出时使用变量方式。 ○ *T*：三倍长的3DES算法密钥，LMK加密输出时使用变量方式。 ○ *X*：双倍长的3DES算法密钥。 ○ *Y*：三倍长的3DES算法密钥。 ○ *P*：SM1算法密钥。 ○ *R*：SM4算法密钥。 ○ *L*：AES-128算法密钥。 ○ *M*：AES-192算法密钥。 ○ *N*：AES-256算法密钥。
密钥类型	不同密钥类型具有不同的用途。
存储到密码机内索引	生成的密钥是否存储到密码机索引。
密钥索引	选中**存储到密码机内索引**后，设置索引号。 取值范围：1~2048
密钥标签	用于在密钥内部存储时标记密钥的标签说明。
LMK加密的新密钥密文	生成的密钥密文。
新密钥校验码	新密钥的校验码。

5. 单击**产生**。

   产生新的随机密钥并输出显示密文和校验值。

10.7.4.2.6.2. 成份合成密钥

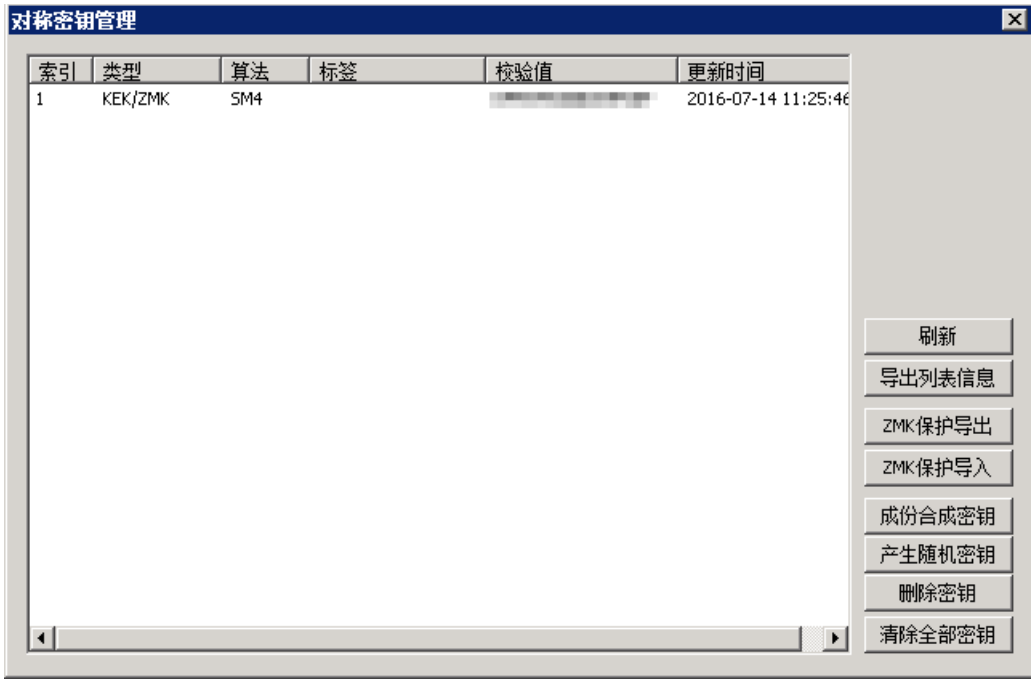
本文介绍了如何成份合成密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

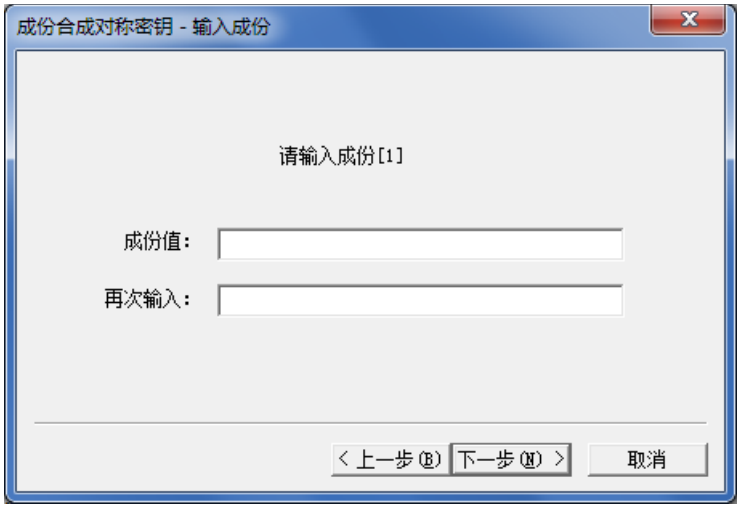
1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



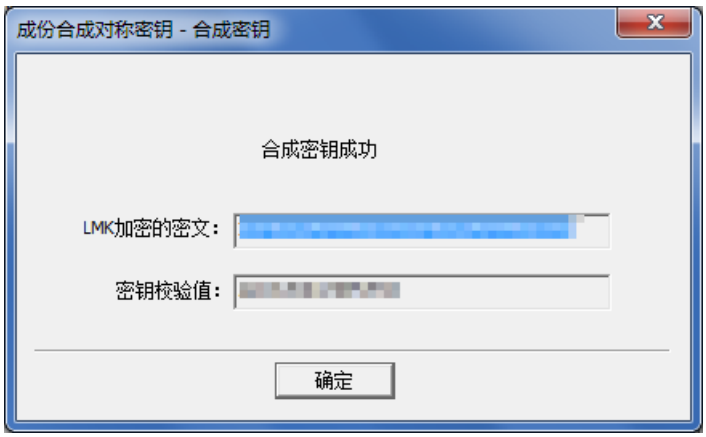
3. 单击**成份合成密钥**。
4. 在对话框中配置参数，单击**下一步**。



5. 依次输入密钥成份，单击**下一步**。



所有成份全部输入后，合成新的密钥并显示密文和校验值。



6. 单击**确定**。

10.7.4.2.6.3. 删除密钥

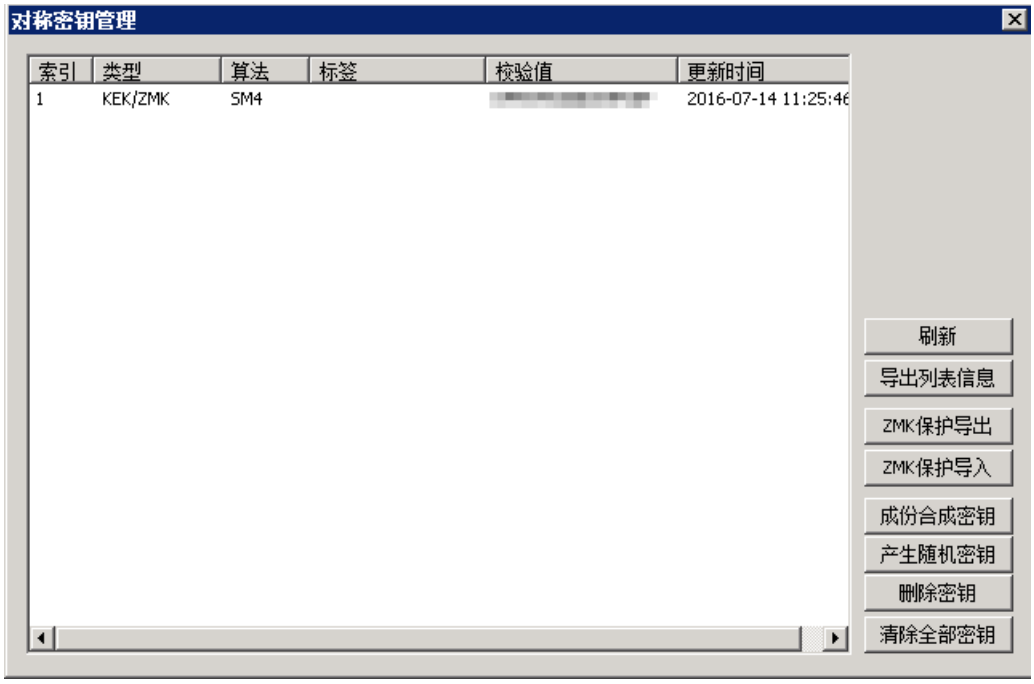
本文介绍了如何删除密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 在左侧列表中选择密钥。
4. 单击**删除密钥**。
5. 在确认提示框中，单击**是**。

10.7.4.2.6.4. 清除全部密钥

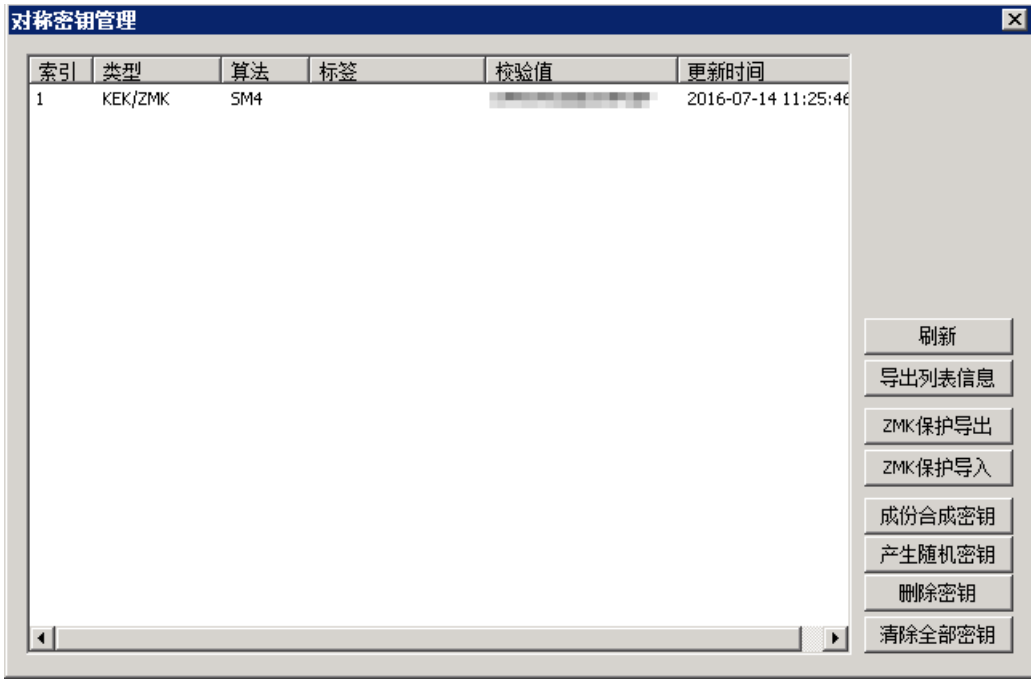
本文介绍了如何清除全部密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 单击**清除全部密钥**。
4. 在确认提示框中，单击**是**。

10.7.4.2.6.5. 导出列表信息

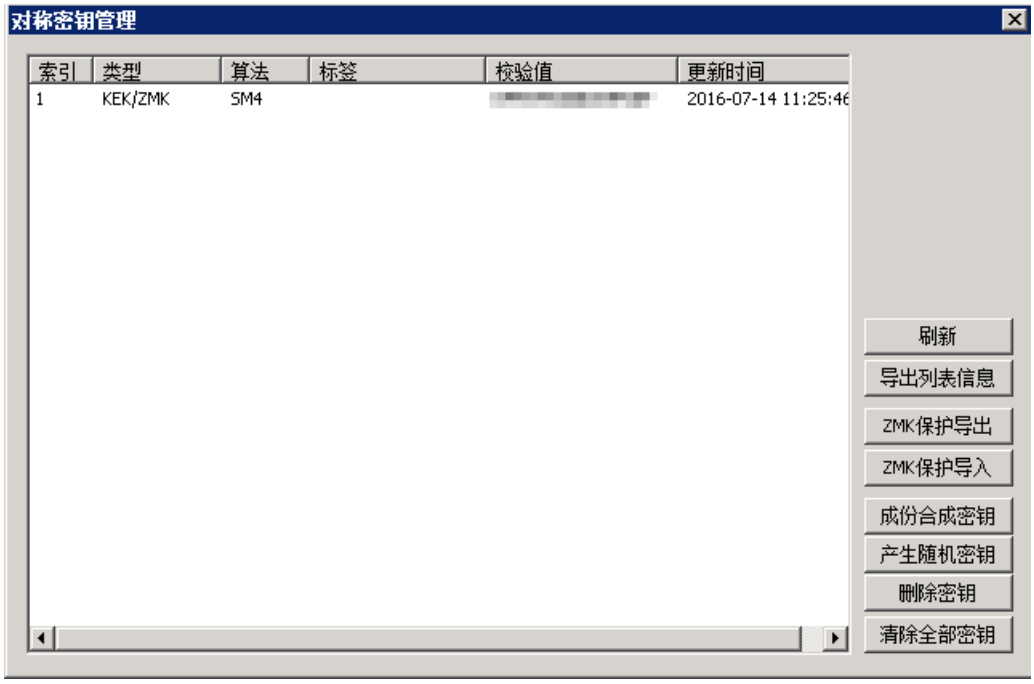
本文介绍了如何导出对称密钥的列表信息。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 单击**导出列表信息**。

   对称密钥列表中所有信息将采用追加模式导出到*keylist.txt*，文件位于*VsmManager.exe*所在目录。

10.7.4.2.6.6. ZMK保护导出

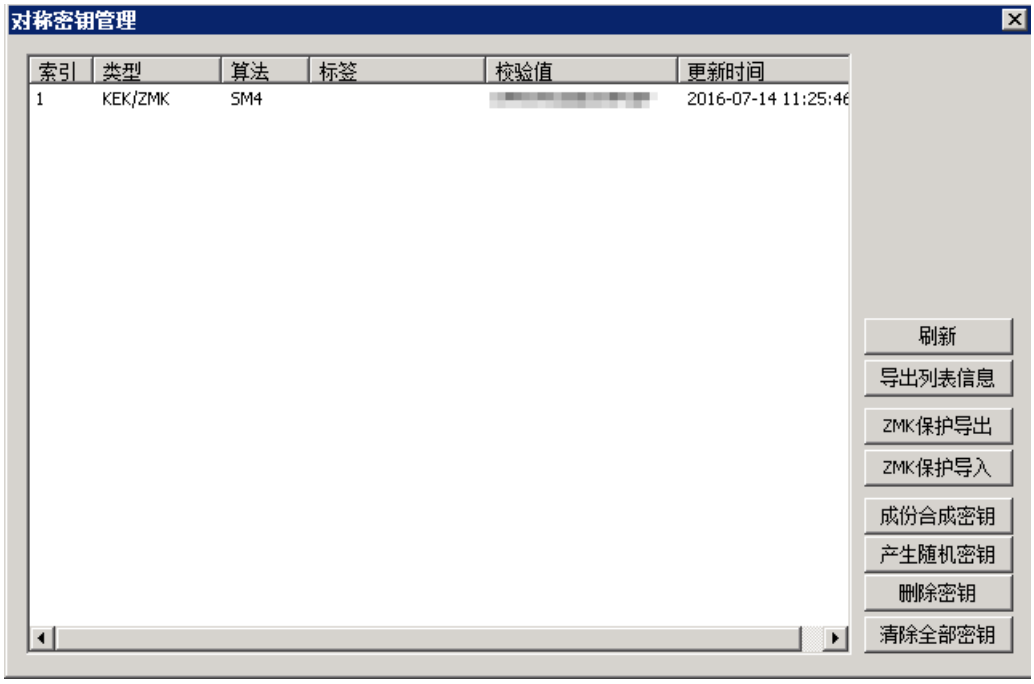
本文介绍了如何ZMK保护导出。

背景信息

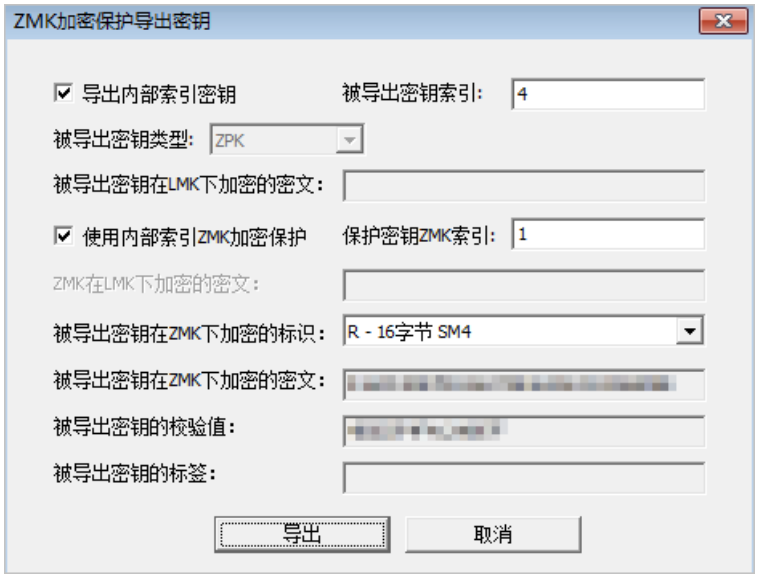
支持通过ZMK保护导出加密机内密钥或者外部输入的在LMK下加密的密文。

操作步骤

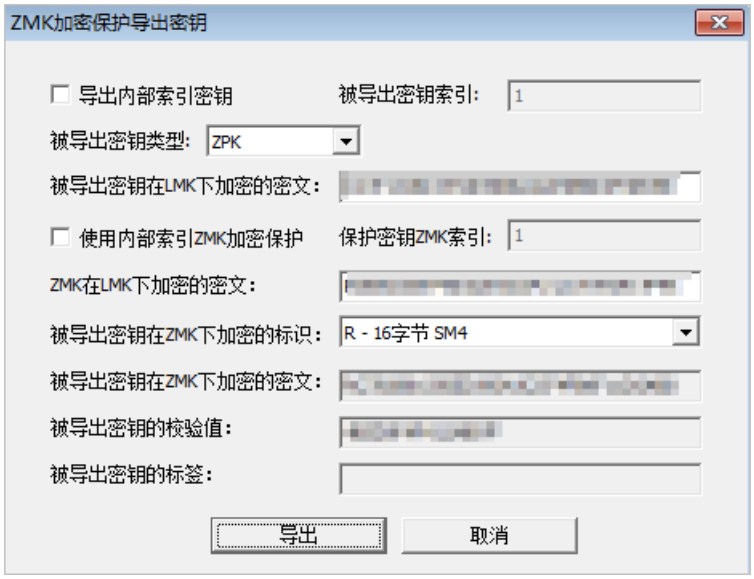
1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 在左侧列表中选择密钥。
4. 单击**ZMK保护导出**。
5. 配置ZMK保护导出方式。
   - 使用密码机内存储的ZMK。



   - 使用外部输入的ZMK。



> 说明
>
> **被导出密钥在ZMK下加密的标识**需要选择正确，否则导出失败。
>
> 例如需要导出的密钥加密时使用的加密标识为*R - 16字节 SM4*，则**被导出密钥在ZMK下加密的标识**也需要选择*R - 16字节 SM4*。

6. 单击**导出**。

10.7.4.2.6.7. ZMK保护导入

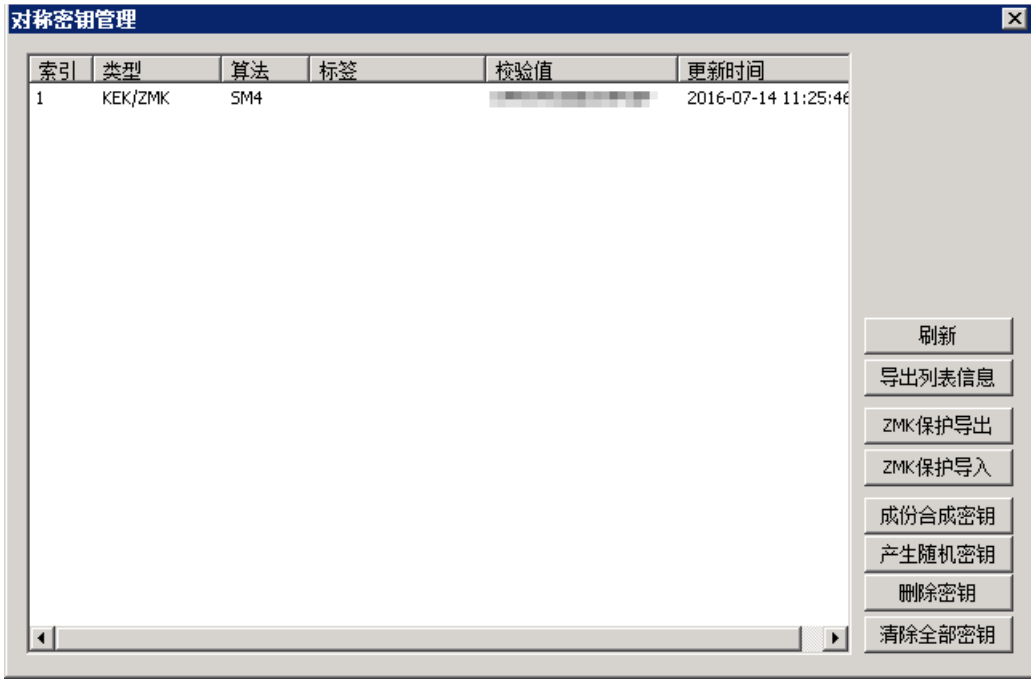
本文介绍了如何ZMK保护导入。

背景信息

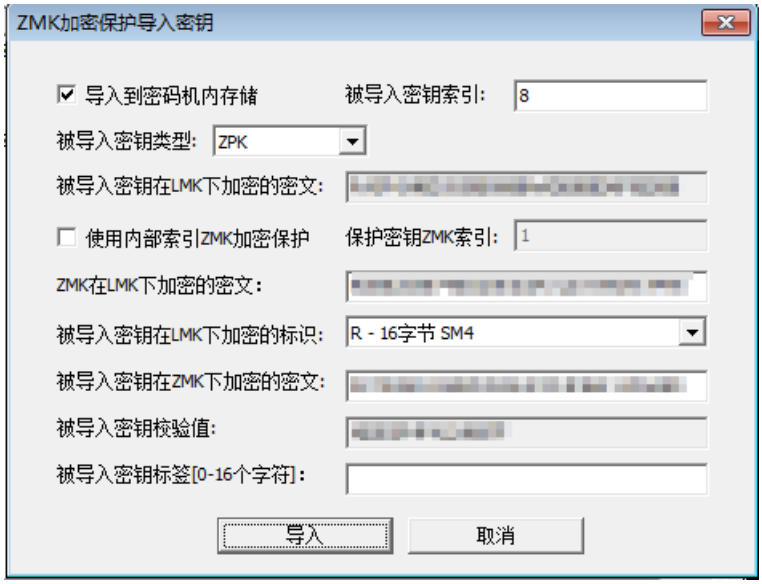
支持通过ZMK保护导入外部输入的在ZMK下加密的密钥密文并可选的存储到密码机。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**密钥管理 > 管理对称密钥**。



3. 单击**ZMK保护导入**。
4. 配置导入信息。



5. 单击**导入**。

10.7.4.2.7. 非对称密钥管理

10.7.4.2.7.1. 产生随机密钥

该章节介绍了如何产生随机密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

背景信息

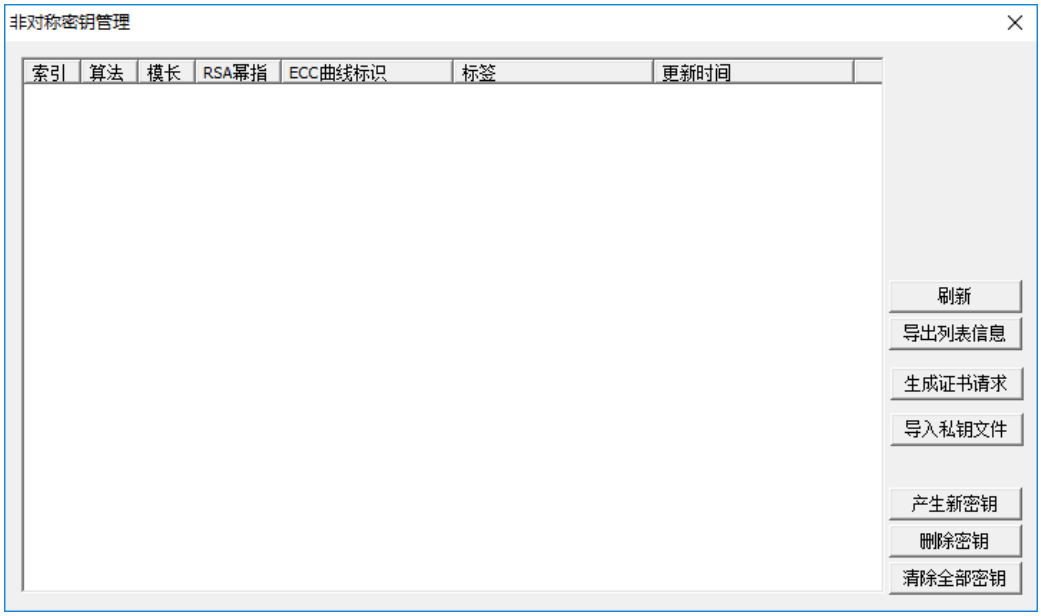
非对称密钥状态信息如下表所示。

非对称密钥状态信息

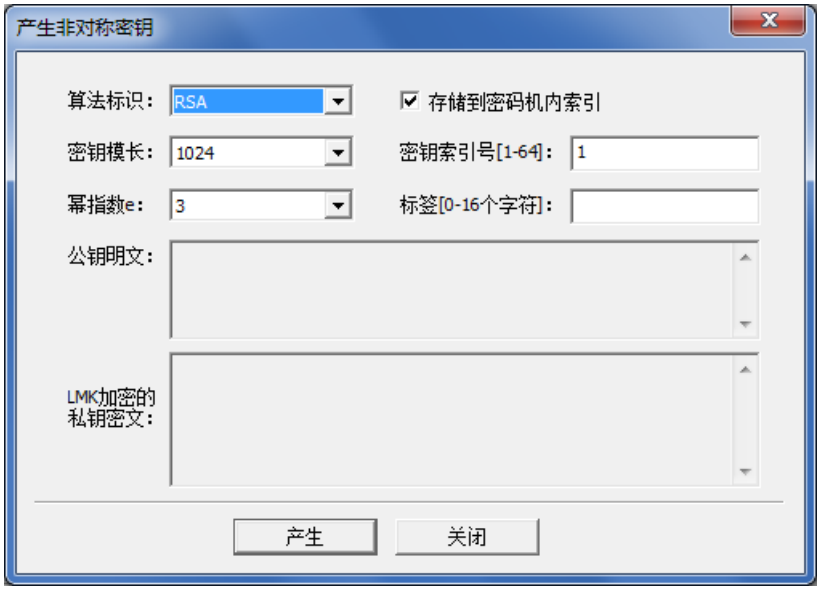
信息	说明
密钥索引号	非对称密钥索引号范围1~64，RSA和SM2密钥各自独立编号
密钥算法	RSA、ECC
模长	• RSA算法：模长支持1024、1152、1408、1912、2048位 • ECC算法：模长支持256位
RSA幂指	仅对RSA算法有效，支持3、65537
ECC曲线标识	仅对ECC算法有效，支持SM2_OSCCA_NEWFP_256曲线
密钥标签	用户自定义的密钥标识，0~16个字符
更新时间	密钥产生或导入的时间

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 管理非对称密钥** 。



3. 单击**产生随机密钥**。
4. 在对话框中配置参数。



5. 单击**产生**。

   产生新的非对称密钥并输出显示公钥明文和私钥密文。

10.7.4.2.7.2. 删除密钥

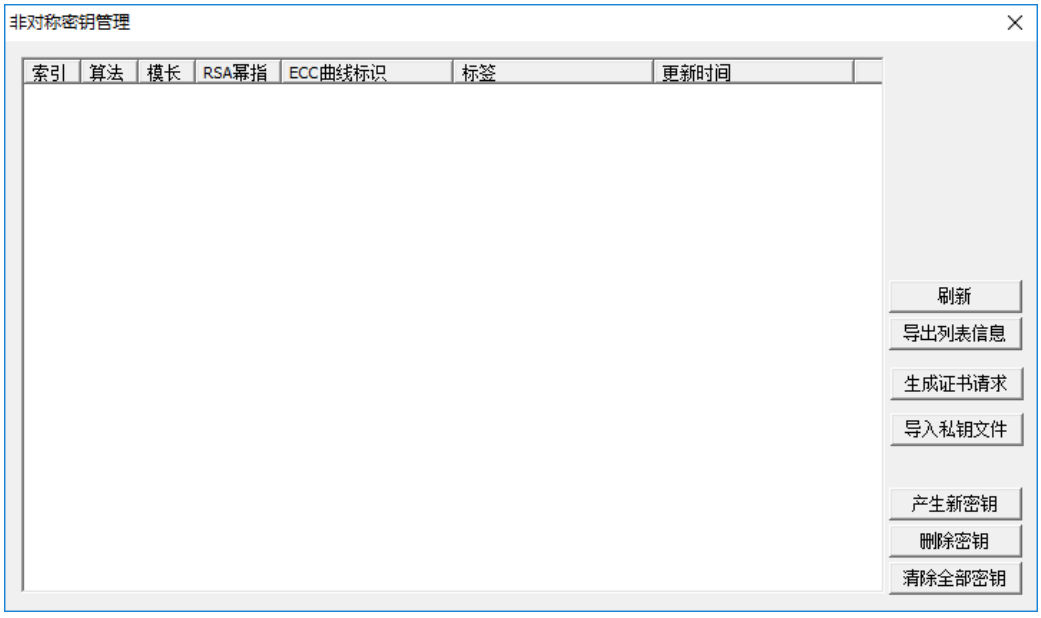
该章节介绍了如何删除密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 管理非对称密钥** 。



3. 在左侧列表中选择密钥。

4. 单击**删除密钥**。
5. 在确认提示框中，单击**是**。

10.7.4.2.7.3. 清除全部密钥

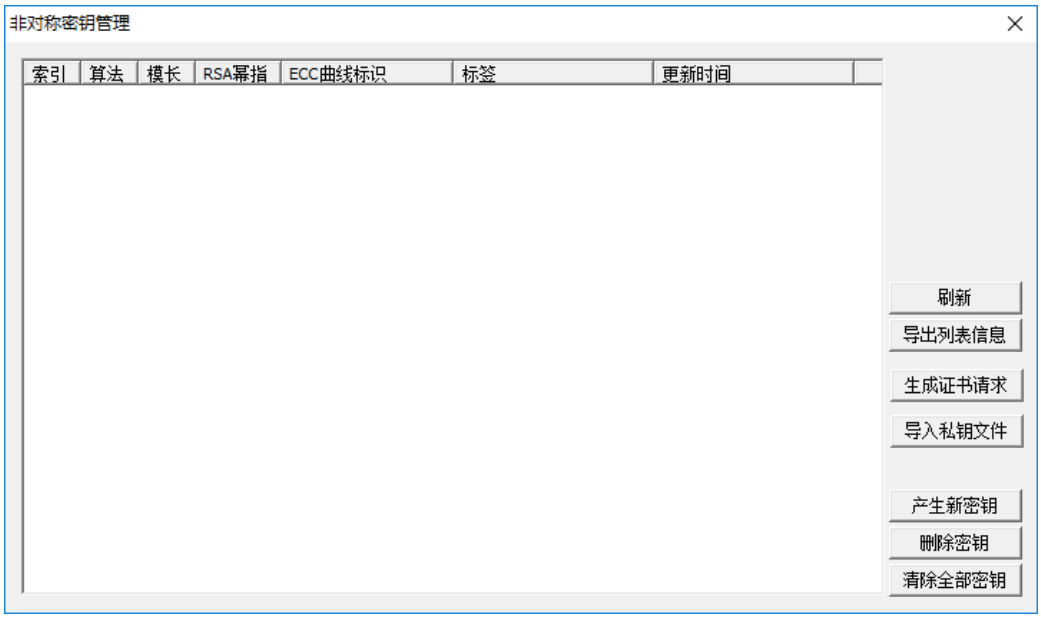
该章节介绍了如何清除全部密钥。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 管理非对称密钥** 。



3. 单击**清除全部密钥**。
4. 在确认提示框中，单击**是**。

10.7.4.2.7.4. 导出列表信息

该章节介绍了如何导出对称密钥的列表信息。

前提条件

需要获取**应用密钥管理**的授权许可，具体操作，请参见授权操作。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 管理非对称密钥** 。



3. 单击**导出列表信息**。

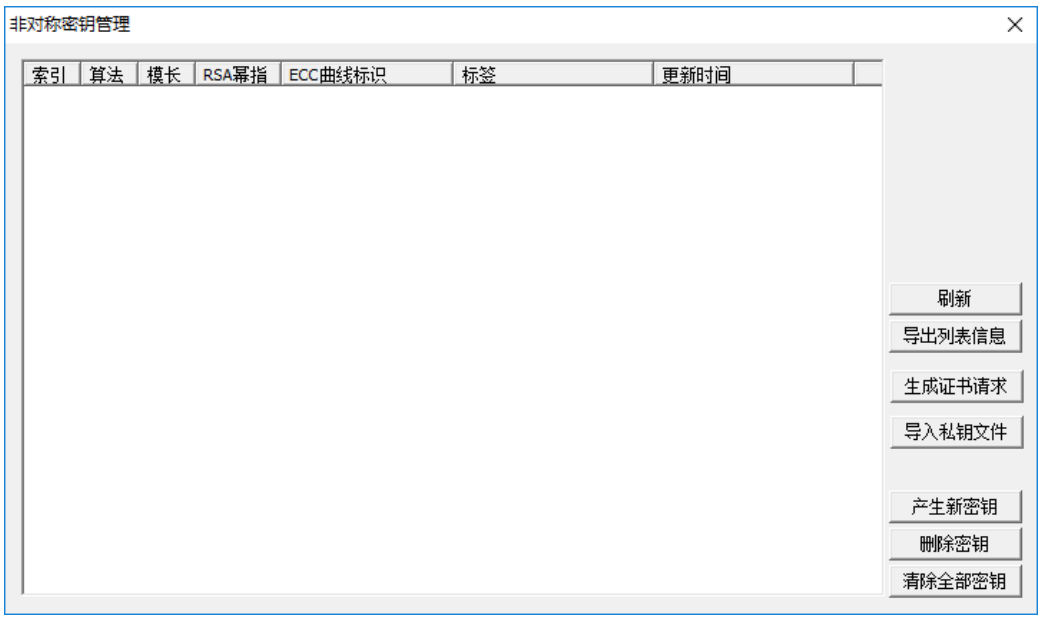
   非对称密钥列表中所有信息将采用追加模式导出到*keylist.txt*，文件位于*VsmManager.exe*所在目录。

10.7.4.2.7.5. 生成证书请求

该章节介绍了如何生成证书请求。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 管理非对称密钥** 。



3. 单击**生成证书请求**。
4. 配置证书申请请求。



i. 输入合法的主题，例如：/CN=XXX。

ii. 选择私钥。

支持密码机内部私钥索引，或者外部输入LMK加密的私钥密文。

- 使用密码机内部私钥索引：

  勾选**是否使用内部索引**，并在**密钥索引**中输入索引号。

- 使用外部输入LMK加密的私钥密文：

  取消勾选**是否使用内部索引**，并在**LMK加密的私钥密文**中输入私钥密文。

5. 单击**确定**。

   在**P10请求**中生成证书信息。

10.7.4.2.7.6. 导入私钥文件

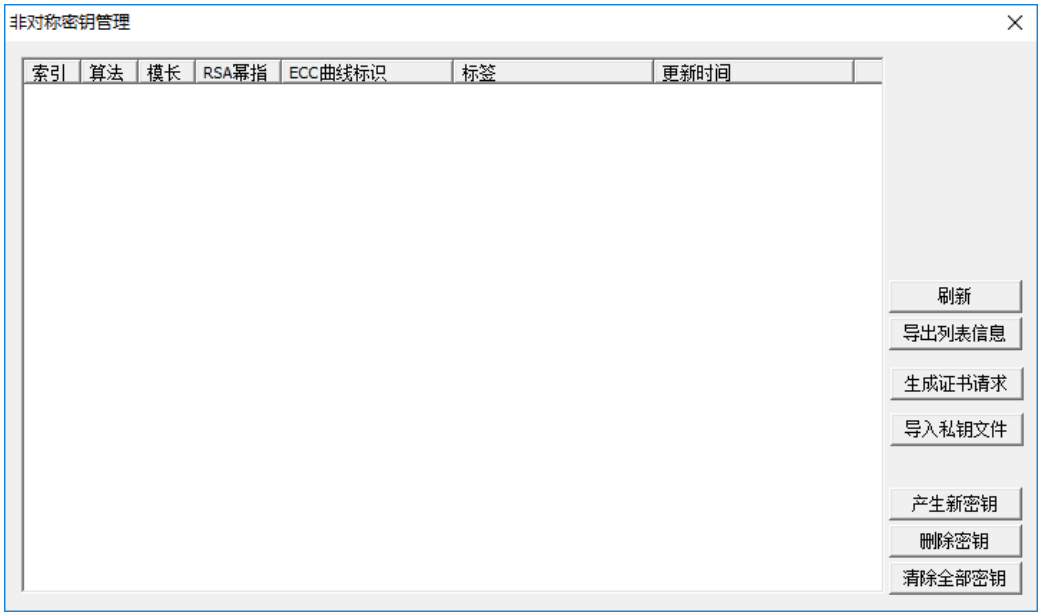
该章节介绍了如何导入私钥文件。

背景信息

支持导入RSA密钥的pfx和pem文件到密码机中保存。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 管理非对称密钥** 。



3. 单击**导入私钥文件**。
4. 选择私钥文件，输入证书口令。



5. 单击**确定**。

10.7.4.2.8. 备份与恢复

10.7.4.2.8.1. 备份密钥

该章节介绍了如何备份密钥。密钥备份，是将密码机内部存储的全部应用密钥（包括对称和非对称密钥）以安全的方式备份导出，然后通过密钥恢复导入到其他密码机中。可用于做多机密钥同步或设备误操作后恢复应用密钥。

背景信息

备份密钥功能需要获取**应用密钥管理**的授权许可，具体操作参见授权操作。

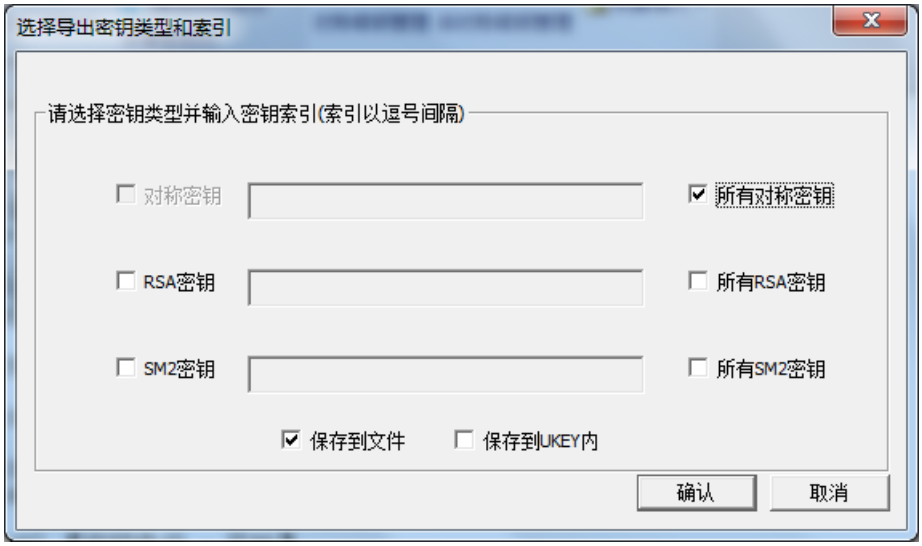
备份密钥可以保存到密钥备份文件或者密钥存储UKEY中。

- 保存到密钥备份文件：备份导出密钥密文存储到用户选定的密钥备份文件中。
- 保存到UKEY中：备份密钥保存在密钥存储UKEY中。

> **说明** 3份密钥备份密钥UKEY（KBKUKEY）、备份文件（或备份密钥UKEY）需妥善保管，待密钥恢复时使用。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 备份导出** 。



3. 设置备份密钥信息，单击**确认**。

   配置信息说明

配置项	说明
导出备份密钥类型	○ 备份指定密钥：选择密钥类型，并输入密钥索引。 密钥索引格式为：`num,num-num`，例如`1,2,4-7`，等同于`1,2,4,5,6,7`。 ○ 备份全部密钥：选择**所有对称密钥**、**所有RSA密钥**、**所有SM2密钥**。
选择保存类型	○ **保存到文件**：备份导出密钥密文存储到用户选定的密钥备份文件中。 ○ **保存到UKEY内**：备份密钥保存在密钥存储UKEY中。

4. 制作3份密钥备份密钥UKEY（KBKUKEY），单击**下一步**。
   i. PC插入空UKEY。

ii. 在**UKEY操作**中，单击**下一步**。

iii. 选择空UKEY，单击**确定**，输入UKEY口令。

iv. 根据步骤~步骤，依次制作3份KBKUKEY。

3份KBKUKEY分给3位密钥管理员保存。

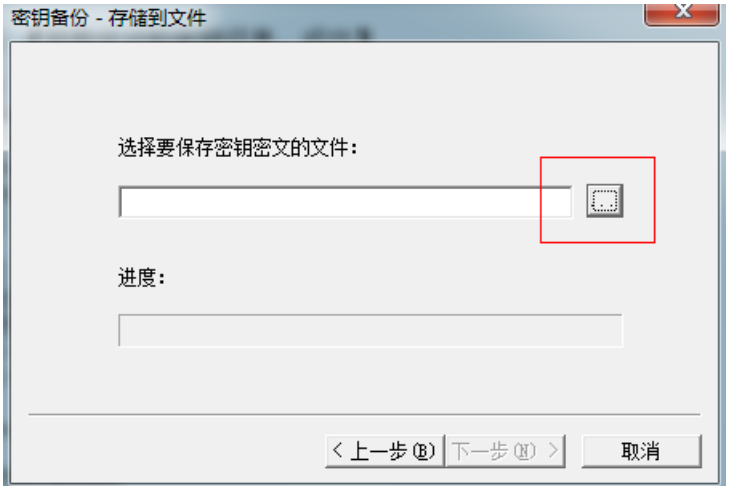
根据保存类型，选择下一步操作。

- 如果是**保存到文件**，跳转到步骤。
- 如果是**保存到UKEY内**，跳转到步骤。

5. （可选）备份密钥保存到文件。

备份密钥数据选择**保存到文件**使用本步骤。

i. 设置密钥备份文件的路径和名称。



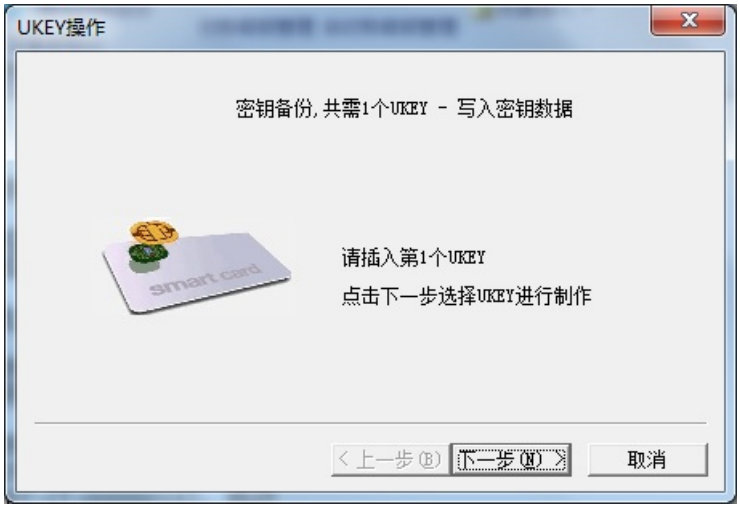
ii. 单击**完成**。

进度条显示备份进度情况，完成后系统显示结果。

6. （可选）备份密钥保存到密钥存储UKEY内。

备份密钥数据选择**保存到UKEY内**使用本步骤。

i. 插入空UKEY，单击**下一步**。



ii. 选择空UKEY，单击**确定**，输入UKEY口令。

iii. 单击**完成**，结束密钥备份。

10.7.4.2.8.2. 恢复密钥

该章节介绍了如何恢复密钥。

操作步骤

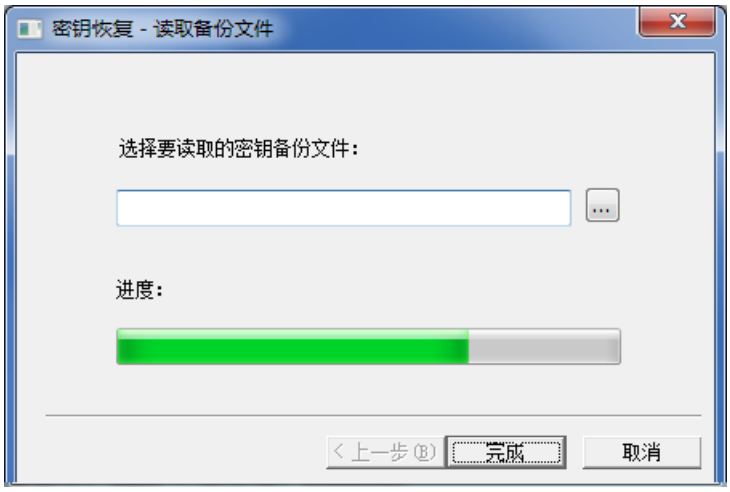
1. 登录VsmManager管理工具。
2. 单击**密钥管理 > 恢复导入** 。
3. 选择恢复来源。
   - 从密钥备份文件中恢复，跳转到步骤。
   - 从密钥存储UKEY中恢复，跳转到步骤。
4. 从密钥备份文件中恢复密钥。

   密钥恢复需使用备份时制作的任意2个KBKUKEY和密钥备份文件。

   i. 单击**从文件中恢复密钥**。

   ii. 插入任意2个KBKUKEY，输入口令，单击**下一步**。

   iii. 选择需要恢复的密钥备份文件。



   iv. 单击**完成**。
5. 从密钥存储UKEY中恢复密钥。

   i. 单击**从UKEY中恢复**。

   ii. 插入任意2个KBKUKEY，输入口令，单击**下一步**。

   iii. 插入密钥存储UKEY，恢复密钥。

10.7.4.3. 设备管理

10.7.4.3.1. 配置主机端口属性

本文介绍如何配置主机端口属性。

背景信息

密码机和ECS之间的服务通讯方式出厂默认配置为明文通讯。

若要配置为密文通讯，则主机端口属性需要设置为*密文通讯*，同时还需要在TACSP安全代理软件进行相应的配置，以保证应用能够正常调用密码服务。密文通讯服务配置，参见配置密文通讯。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**设备管理 > 主机服务端口属性**。
3. 设置主机端口属性。

> **说明** 需要根据实际需求正确配置主机端口属性。



主机端口属性

属性	说明
Socket KeepAlive时间	TCP连接保活探测时间，单位：秒。 取值范围：60~600
消息报文头长度	主机报文消息头长度，单位：字节。 取值范围：60~600
消息报文编码格式	主机报文的编码格式。 ○ ASCII ○ EBCDIC
主机服务通讯方式	○ 明文通讯：与主机服务间的通讯为明文。 ○ 密文通讯：与主机服务间的通讯为密文。

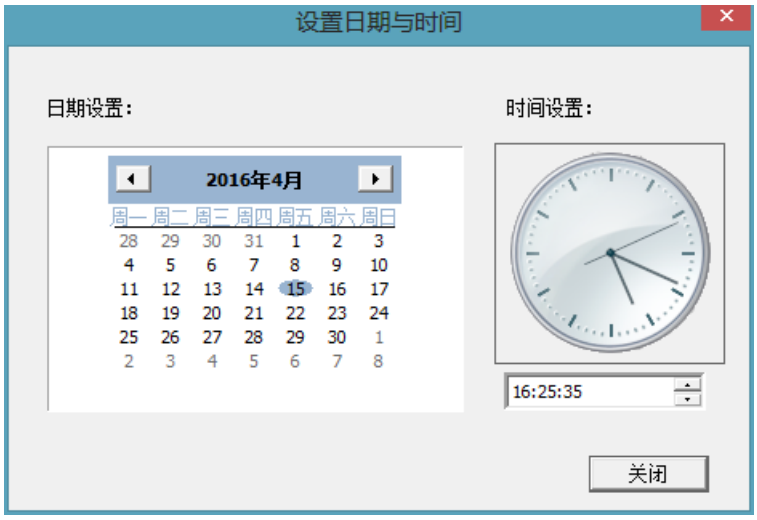
10.7.4.3.2. 配置设备时间

该章节介绍如何配置设备时间。

操作步骤

1. 登录VsmManager管理工具。

2. 单击**设备管理 > 设备时间** 。
3. 设置时间和日期。



10.7.4.3.3. 授权管理

10.7.4.3.3.1. 授权操作

本文介绍如何进行授权。

背景信息

部分设备管理操作和主机指令应用需要获取授权许可，密码机支持严格灵活的授权管理控制。授权具有以下优点：

- 授权机制可配置

  支持1选1、3选2、5选3和无授权控制机制。授权控制机制需在初始化的过程中设置，完成初始化后不允许被修改。

- UKEY授权机制

  通过验证授权UKEY完成对授权人员的身份识别，安全可靠。

- 分类分时授权控制

  通过授权UKEY验证后，可选择本次授权的操作类别及给予授权的时间，当某类操作授权的时效过期后，其授权许可将自动失效。

> **说明** 初始化时，如果**授权机制**配置为*无授权控制机制*，所有的操作均不受限。则本文不需要设置。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**设备管理 > 操作授权**。
3. 根据提示依次插入授权UKEY，输入口令，单击**下一步**。

   系统将根据授权机制要求半数以上的授权UKEY验证通过。授权UKEY的验证次序无关，但重复验证无

效。

4. 配置授权操作信息。

   可同时为多个类别授权不同的时限。



   授权类别说明

主类	子类	操作范围说明
设备管理	设备配置更新	重置端口属性，包括主机服务端口。
	应用密钥管理	○ 随机产生内部存储的密钥。 ○ 成份形式合成对称密钥。 ○ 删除内部对称或非对称密钥。 ○ 清除内部对称或非对称密钥。 ○ 内部密钥备份导出。
主机服务	账户PIN解密	使用BA、NG主机命令。
	产生公钥MAC	使用EO、TQ主机命令。
	内部密钥更新	○ KR、KD、KI、SI、TW、TY，内部存储模式的对称密钥的产生或导入。 ○ EI、EK、EJ、TS，内部存储模式的RSA密钥对的产生或导入。 ○ E0、E1、TU，内部存储模式的SM2密钥对的产生或导入。

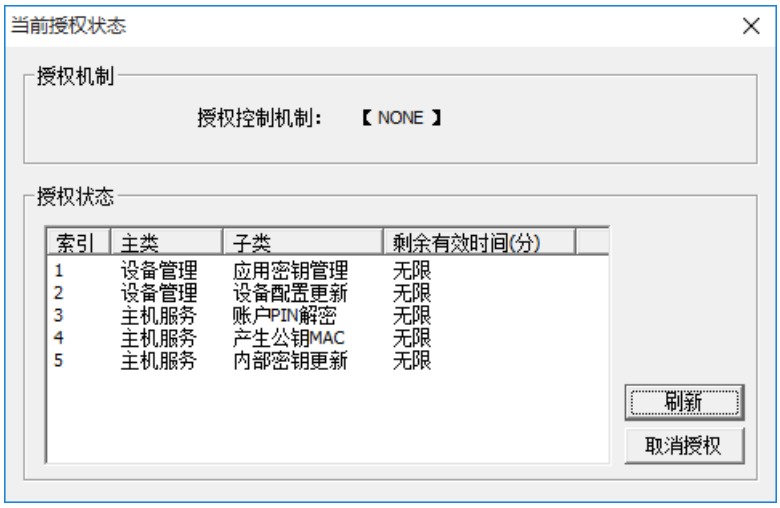
5. 单击完成。

10.7.4.3.3.2. 获取授权状态

该章节介绍如何获取授权状态。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > 当前授权状态** 。
3. 查看授权状态信息。



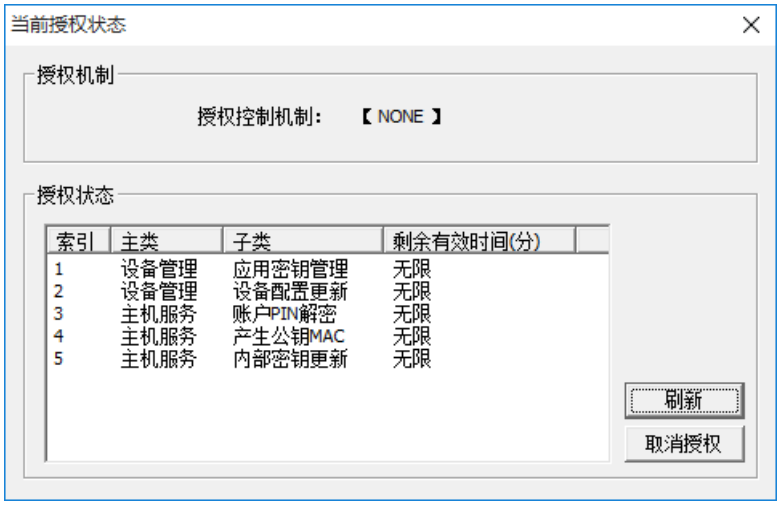
4. 单击**刷新**。

10.7.4.3.3.3. 取消授权

该章节介绍如何取消授权。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > 当前授权状态** 。
3. 在**授权状态**中选择授权类型。



4. 单击**取消授权**。

10.7.4.3.3.4. 签发应用许可

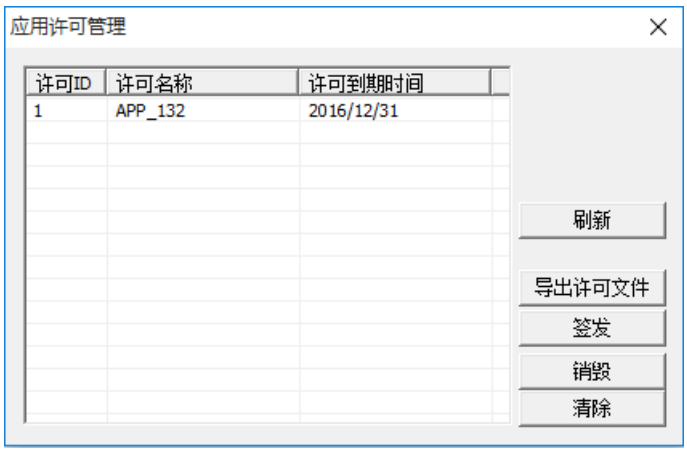
本文介绍如何签发应用许可。

背景信息

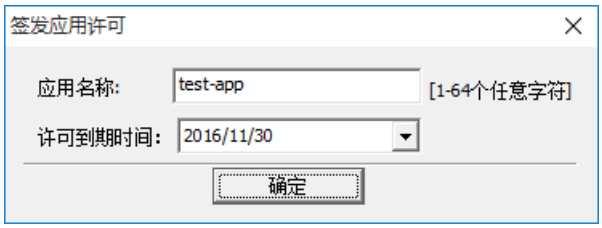
配置密文通讯时，需要为TACSP签发应用许可。

操作步骤

1. 登录VsmManager管理工具。
2. 选择**设备管理 > 应用许可管理**。
3. 单击**签发**。



4. 设置应用名称和到期时间。



5. 单击**确定**。

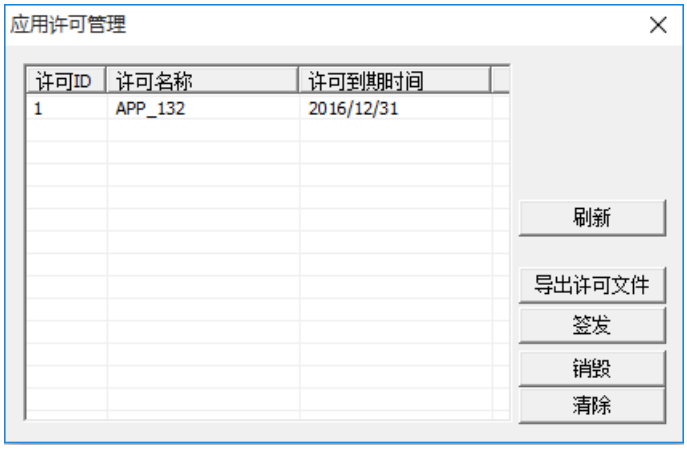
   生成应用许可文件（*.license*后缀的文件），并自动导出到VsmManager管理工具所在目录。

10.7.4.3.3.5. 管理应用许可

该章节介绍如何管理应用许可。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > 应用许可管理** 。
3. 查看应用许可列表。



4. 管理应用许可。
   - **导出许可文件**

     选择列表中已有的应用许可，单击**导出许可文件**，应用许可文件导出到VsmManager管理工具所在目录。
   - **销毁**

     选择列表中已有的应用许可，单击**销毁**，应用许可文件将失效。
   - **清除**

     单击**清除**，所有应用许可文件将失效。

10.7.4.3.4. UKEY管理

10.7.4.3.4.1. 概述

该章节介绍UKEY的管理规则和分类。

UKEY管理操作不需要登录密码机即可执行，用户可根据系统的安全需求制定相应的UKEY管理规则，例如：

- 定义UKEY持有人和UKEY类型。
- UKEY进行格式化（个人化）操作。
- 重置用户标识。

UKEY分类说明参见UKEY分类说明。所有的UKEY在首次使用时，均需要输入保护口令。

UKEY分类说明

UKEY类别	说明	用途
主密钥成份UKEY	保存用户输入的设备主密钥DMK成份数据。	用于合成设备主密钥。
授权UKEY	保存设备授权信息数据。	用于授权管理的身份验证。
密钥备份密钥UKEY	保存密钥备份密钥KBK以秘密共享算法（2 of 3）分割后的秘密成份。	恢复密钥时使用任意2个恢复原KBK。
密钥存储UKEY	存储备份的密钥。	存储备份的密钥。

UKEY类别	说明	用途
管理员UKEY	存储平台公钥，加密机信息等。	用户开机，协商通讯，以及整个管理工具与密码机通讯运算。

10.7.4.3.4.2. 添加管理员

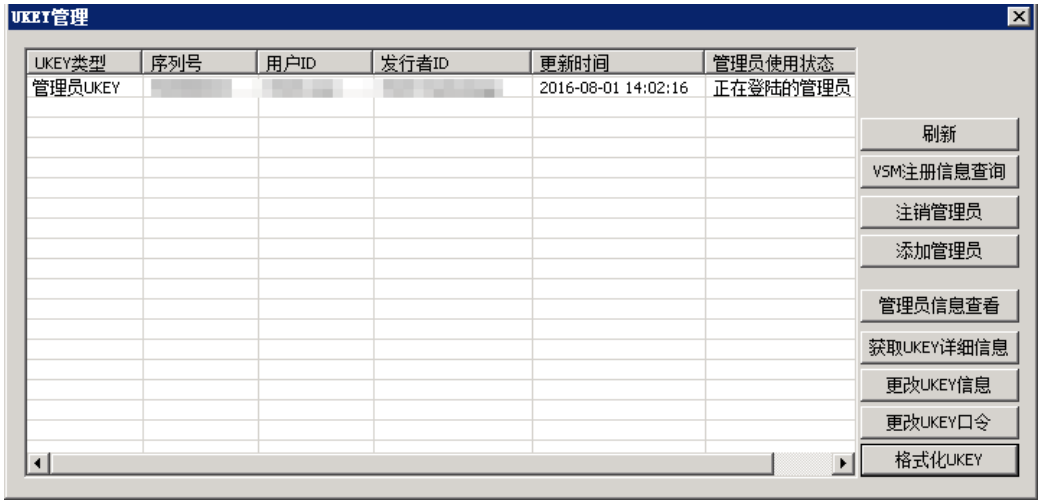
该章节介绍如何添加管理员。

背景信息

首次注册管理员请参考注册管理员UKEY。为了防止管理员UKEY丢失，建议另外添加几把管理员UKEY。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。
3. PC插入空UKEY。
4. 在左侧列表中，选中空UKEY。



5. 单击**添加管理员**。

10.7.4.3.4.3. 注销管理员

该章节介绍如何注销管理员。

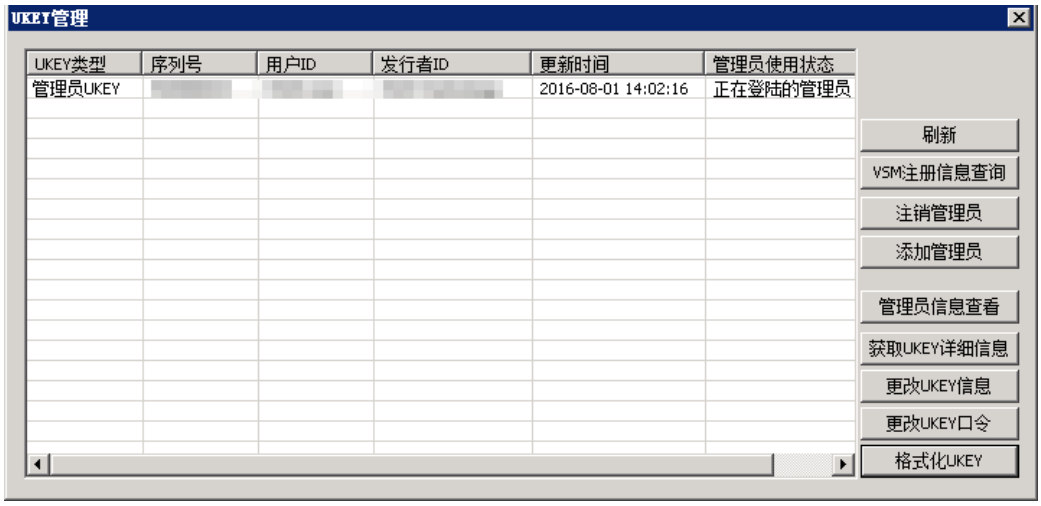
背景信息

> **说明** 只有选择正在登录的管理员UKEY，**注销管理员**操作才能生效。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。

3. 在左侧列表中，选中正在登录的管理员UKEY。



4. 单击**注销管理员**。

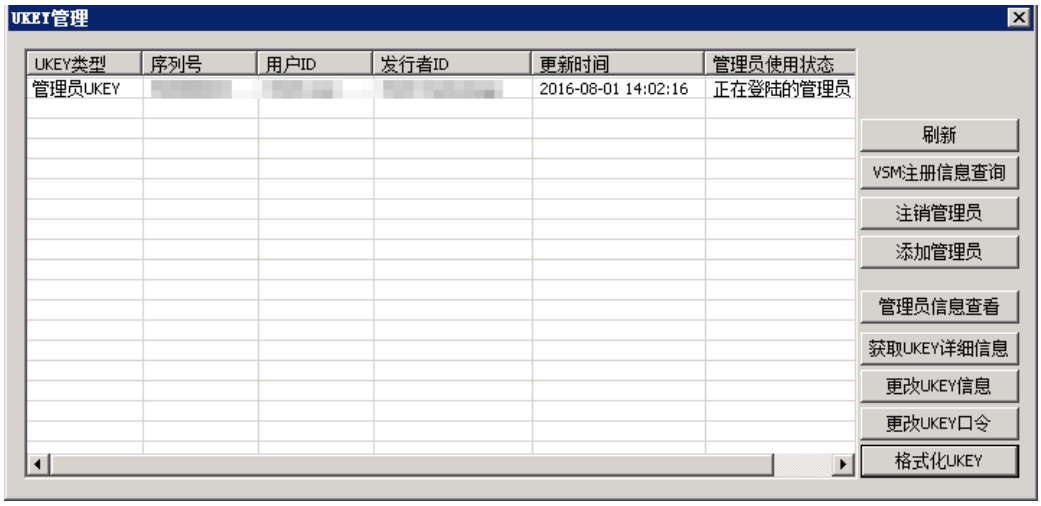
   注销成功后，VsmManager管理工具自动退出。

10.7.4.3.4.4. 查询已注册的管理员UKEY信息

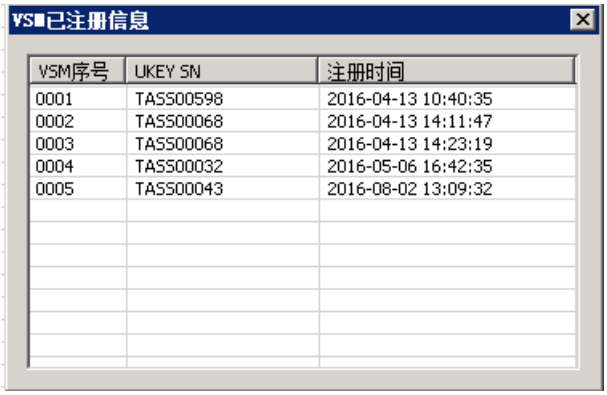
该章节介绍如何查询已注册的管理员UKEY信息。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。
3. 单击**VSM注册信息查询**。



4. 查看已注册的管理员UKEY信息。

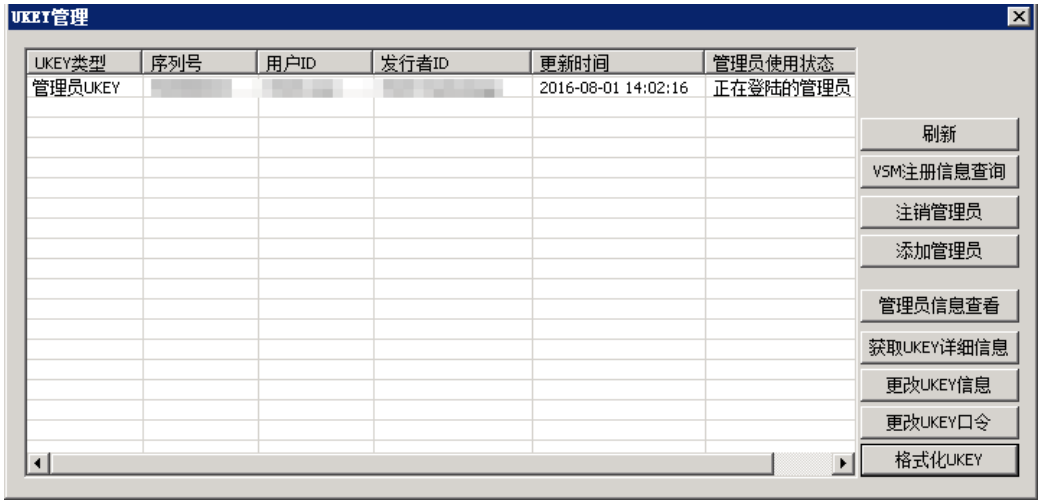


10.7.4.3.4.5. 获取UKEY详细信息

该章节介绍如何获取UKEY详细信息。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。
3. 在左侧选择UKEY，单击**获取UKEY详细信息**。



4. 查看UKEY详细信息。

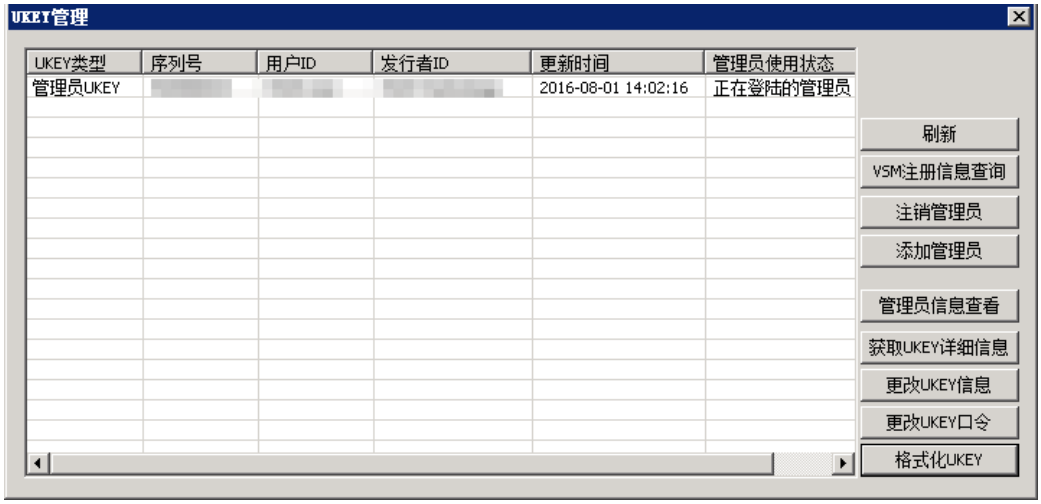
```
[2015-03-04 17:59:47] 【获取UKEY信息,
# UKEY序号  : T-00000015
# UKEY类型  : 密钥存储UKEY
# 格式化时间: 2015-02-09 17:18:00
# 制UKEY时间: 2015-03-04 17:01:20
# 持有人ID  : TASS_MXL
# 发行者ID  : TASS_TECHNOLOGY
# 密钥存储UKEY标识 : 0
```

10.7.4.3.4.6. 更改UKEY信息

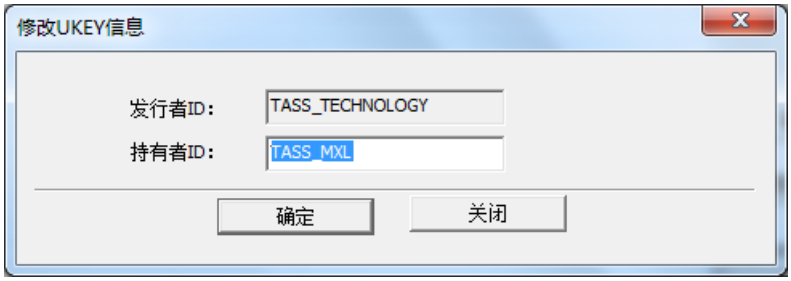
该章节介绍如何更改UKEY信息。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。
3. 在左侧选择UKEY，单击**更改UKEY信息**。



4. 修改**持有者ID**。



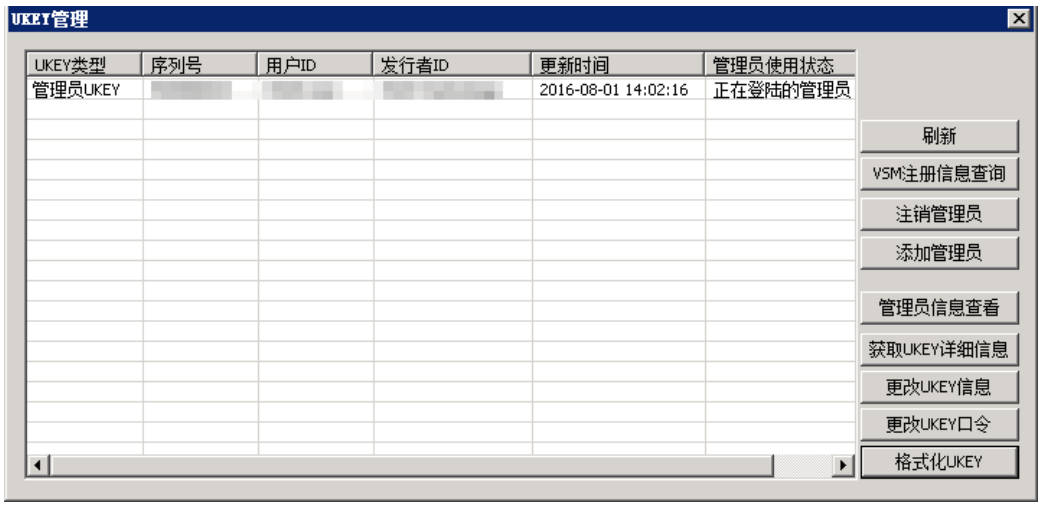
5. 单击**确定**。

10.7.4.3.4.7. 更改UKEY口令

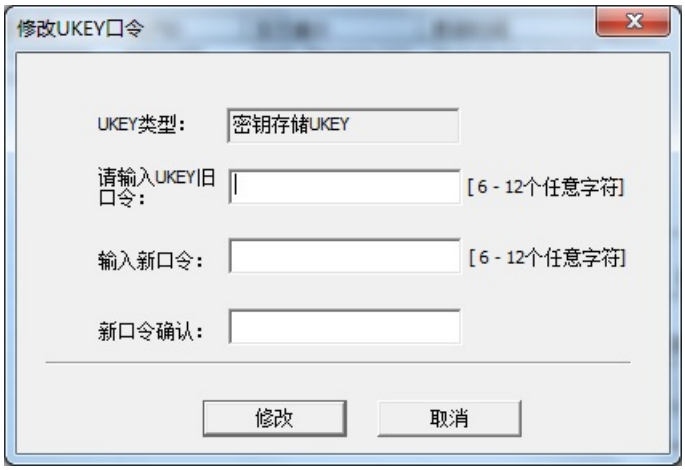
该章节介绍如何更改UKEY口令。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。
3. 在左侧选择UKEY，单击**更改UKEY口令**。



4. 修改UKEY口令。



5. 单击**修改**。

10.7.4.3.4.8. 格式化UKEY

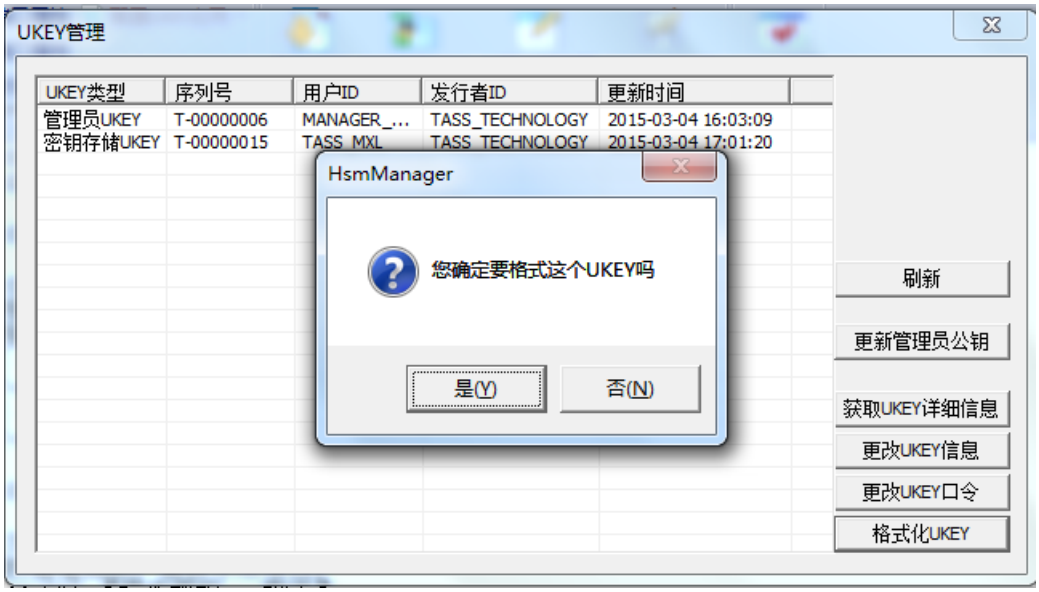
该章节介绍如何格式化UKEY。

背景信息

> **说明** 管理员UKEY不允许格式化。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备管理 > UKEY管理** 。
3. 在左侧选择UKEY，单击**格式化UKEY**。



4. 在确认提示框中，单击**是**。

   格式化后，UKEY内容重置为默认值（空UKEY）。

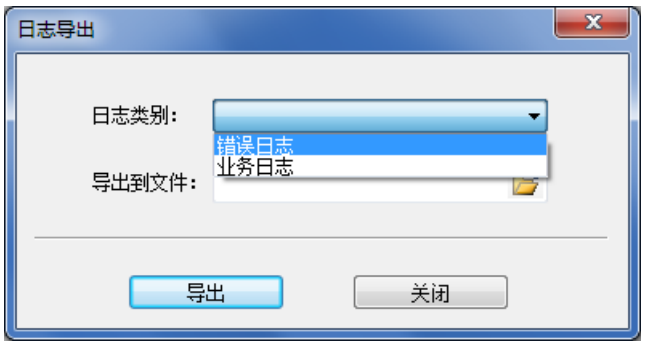
10.7.4.3.5. 设备诊断维护

10.7.4.3.5.1. 导出日志

该章节介绍如何导出日志。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备诊断维护 > 导出日志** 。
3. 设置日志导出信息。



日志导出

参数	说明

参数	说明
日志类别	导出日志类别： ○ 错误日志 ○ 业务日志
导出到文件	选择导出日志保存在本地的路径和文件名。

4. 单击**导出**。

10.7.4.3.5.2. 清除日志

该章节介绍如何清除日志。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备诊断维护 > 清除日志** 。
3. 在确认提示框中，单击**是**。

   操作完成后，密码机将清除全部日志。

10.7.4.3.5.3. 查看设备基础信息

该章节介绍如何查看设备基础信息。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备诊断维护 > 设备基础信息** 。
3. 查看设备基础信息。

```
[2016-04-14 17:22:01] 【获取设备基础信息，成功】
# 设备主密钥校验值: DF0ED66BFA4DC70F
# 主机服务版本号   : H1.24.06
# 管理服务版本号   : M1.17.00
# 加密卡版本号     : C1.16.09
```

10.7.4.3.5.4. 设备自检

该章节介绍如何进行设备自检。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备诊断维护 > 设备自检** 。
3. 检测关键单元情况。

```
[2016-04-14 17:22:22] 【设备自检，成功】
# 物理噪声源检测  : OK
# SM2算法单元检测 : OK
# SM3算法单元检测 : OK
# SM4算法单元检测 : OK
# 密钥库完整性检测: OK
```

10.7.4.3.5.5. 查看主机服务状态

该章节介绍如何查看主机服务状态。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备诊断维护 > 主机服务状态** 。
3. 查看主机服务状态。

```
[2016-04-14 17:22:44] 【获取服务连接状态，完成】
# 主机服务: 正常
# 支持的最大连接数: 64
# 当前已使用连接数: 10
# 剩余可用连接数  : 54
```

10.7.4.3.5.6. 查看设备资源信息

该章节介绍如何查看设备资源信息。

操作步骤

1. 登录VsmManager管理工具。
2. 单击**设备诊断维护 > 设备资源信息** 。
3. 查看设备资源信息。

```
[2016-04-14 17:23:15] 【获取密码机资源占用信息，成功】
# 内存占用率: 7.84%
# CPU占用率 : 0.25%
```

10.7.5. TACSP管理

10.7.5.1. 配置TACSP

本文介绍如何配置TACSP安全代理软件。TACSP安全代理软件基于密码机的安全应用而设计开发的安全代理软件，是集多机热备、负载均衡功能为一体的密码机应用平台。

前提条件

ECS和密码机在同一个VPC网络中。

背景信息

TACSP安全代理软件支持的操作系统和加密方式如下。

- 操作系统：支持Linux、AIX、HP-UNIX等类UNIX操作系统。

- 加密方式：支持以Socket方式提供密码安全服务，应用程序通过Socket方式访问安全代理软件。

操作步骤

1. 通过FTP软件上传TACSP安全代理软件到业务ECS。
2. 通过SSH登录业务ECS。
3. 进入TACSP所在路径。
4. 配置*tacsp_cfg.ini*。

   *tacsp_cfg.ini*配置文件内容如下：

```
[TACSP_IPC]
COMMAND_QUEUE_KEY               = 130
RESPONSE_QUEUE_KEY              = 131
SHARED_MEMORY_KEY               = 132
LOG_LEVEL                       = 1
[TACSP_SERVERINFO]
LISTEN_IP_FLG                   = 0
LISTEN_PORT                     = 9999
HSM_LOADSIZE                    = 2
HSM_LOADSELF                    = 0
[TACSP_HSMINFO]
HSM_COUNT                       = 0
TOTAL_TIMEOUT                   = 6
SINGLEHSM_TIMEOUT               = 2
[TACSP_HSM00]
HSM_TYPE                        = SJJ1310
HSM_IP                          = 192.*.*.51
HSM_PORT                        = 8018
HSM_WEIGHT                      = 10
HSM_ENC_COMM                    = 0
[TACSP_HSM01]
HSM_TYPE                        = SJJ1310
HSM_IP                          = 192.*.*.102
HSM_PORT                        = 8018
HSM_WEIGHT                      = 10
HSM_ENC_COMM                    = 1
```

配置说明

节点	键名	说明
TACSP_IPC	无	TACSP使用的IPC相关ID。
	COMMAND_QUEUE_KEY	TACSP使用2个队列和1个共享内存。 此处配置的队列ID和共享内存ID，必须确保与当前系统中的相关ID不冲突。 取值范围：1~65537
	RESPONSE_QUEUE_KEY	
	SHARED_MEMORY_KEY	

节点	键名	说明
	LOG_LEVEL	日志级别： ○ *0*：不记录任务日志。 ○ *1*：记录错误日志。 ○ *2*：记录连接信息。 ○ *3*：记录调试信息日志。
TACSP_SERVERINFO	无	对外提供Socket服务配置信息。
	LISTEN_IP_FLG	○ *0*：默认值，监听127.0.0.1 ○ *1*：监听0.0.0.0
	LISTEN_PORT	负载热备对外提供的监听端口。 取值范围：1025~65535
	HSM_LOADSIZE	头部中表示报文长度的字节数。
	HSM_LOADSELF	头部表示报文长度中是否包含自身长度： ○ *0*：不包含 ○ *1*：包含
TACSP_HSMINFO	无	密码机相关信息。
	HSM_COUNT	密码机数量。 取值范围：1~20
	TOTAL_TIMEOUT	每次Socket通讯总的超时时间，单位：秒。 建议取值：加密机个数 * 单台加密机通讯超时 + 2
	SINGLEHSM_TIMEOUT	每台加密机每次Socket通讯的超时时间，单位：秒。
TACSP_HSM*xx*	无	某索引密码机的信息，有n个密码机，必须有n个节配置。 *xx*取值范围：00~（n-1）
	HSM_TYPE	密码机类型
	HSM_IP	密码机的IP地址
	HSM_PORT	密码机的端口号

节点	键名	说明
	HSM_WEIGHT	密码机的工作权重，即安全代理软件和此台加密机有多少个Socket连接。 取值范围：1~65
	HSM_ENC_COMM	和密码机的通讯模式： ○ *0*：明文通讯 ○ *1*：密文通讯

5. （可选）配置环境变量TACSPCFG和CLUSTERDEBUG环境变量。

   > **说明** 如不配置TACSPCFG，则配置文件必须在TACSP安全代理软件所在的路径下；如不配置CLUSTERDEBUG，则日志将默认输出在TACSP安全代理软件所在的路径下。

   i. 编辑*/etc/profile*。

   ```
   vi /etc/profile
   ```

   ii. 在*/etc/profile*中添加变量。

   ```
   export TACSPCFG=tacsp_cfg.ini所在目录
   export CLUSTERDEBUG=日志存储目录
   ```

   iii. 使环境变量立即生效。

   ```
   source /etc/profile
   ```

10.7.5.2. 配置密文通讯

本文介绍如何配置密文通讯。

背景信息

密文通讯方式是指应用主机与密码机之间的通讯采用加密的方式，能够在专有云的环境下提供更安全更可靠的加密服务。

操作步骤

1. 配置主机端口属性。

   主机服务通讯方式修改为*密文通讯*。

2. 签发应用许可证。

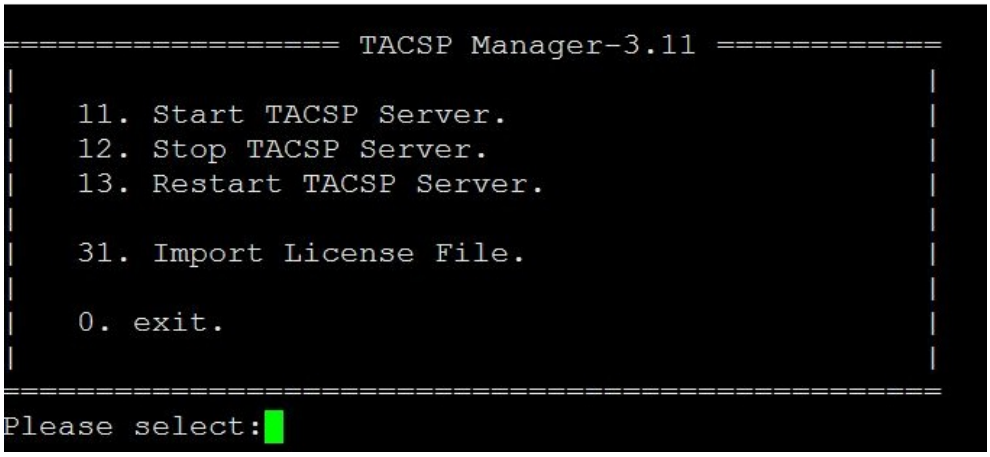
   应用许可的内容包括VSM设备公钥、TACSP公私钥、应用名称、签发时间、到期时间及设备私钥对前述内容的签名。

   > **说明** 如果有多个密码机，分别导出应用许可证。

3. 应用许可证通过FTP上传到TACSP安全代理软件所在路径。
4. 导入应用许可证。

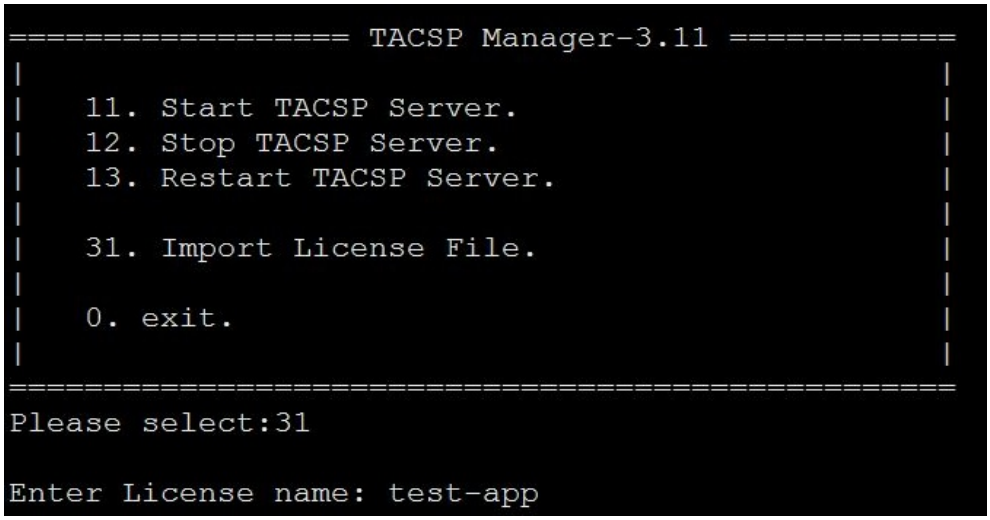
i. SSH登录ECS并进入TACSP安全代理软件所在路径。

ii. 执行./keyMng。



iii. 输入*31*，按回车键（Enter）。

开始导入应用许可证。



iv. 输入许可证名称，按回车键（Enter）。

v. （可选）重复步骤4的c~d步骤，导入其他加密机的应用许可证。

如果有多台密码机，则需要依次导入其他密码机的应用许可证。

vi. 输入*11*，启动TACSP安全代理软件。

如果TACSP已经启动，则输入*13*，重启TACSP。

10.7.5.3. 启动TACSP

该章节介绍如何启动TACSP。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行./keyMng。

4. 输入*11*，按回车键（Enter）。

10.7.5.4. 重启TACSP

该章节介绍如何重启TACSP。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./keyMng**。
4. 输入*13*，按回车键（Enter）。

10.7.5.5. 停止TACSP

该章节介绍如何停止TACSP。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./keyMng**。
4. 输入*12*，按回车键（Enter）。

10.7.5.6. 设置TACSP日志级别

本文介绍如何设置TACSP日志级别。

背景信息

修改TACSP日志级别：

- 未启动TACSP，修改LOG_LEVEL参数值，具体参考配置TACSP。
- 已启动TACSP，可以按照本文修改。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行**./setlog log_level**。

   *log_level*取值如下：

   - *0*：不记录任务日志。
   - *1*：记录错误日志。
   - *2*：记录连接信息。
   - *3*：记录调试信息日志。

10.7.5.7. 停止连接密码机

本文介绍TACSP如何停止连接密码机。

背景信息

在TACSP已经启动成功的情况下，可以单独停止连接某台密码机。此功能适用情况：

- 需要确认密码机无处理中的业务。
- 仅用于替换密码机时使用。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行./keyMng stop ip。

   *ip*为密码机IP地址。

   通过查看*tacsplog*日志文件，确认执行结果是否成功。

10.7.5.8. 启动连接密码机

本文介绍TACSP如何启动连接密码机。

背景信息

在TACSP已经启动成功的情况下，停止连接某台密码机后，可以进行重新连接。此功能适用情况：

- 确认新连接的密码机已经写入配置文件，且TACSP和密码机之间通讯畅通。
- 仅用于动态增加密码机时使用。

操作步骤

1. 通过SSH软件登录ECS。
2. 进入TACSP所在路径。
3. 执行./keyMng start ip。

   *ip*为密码机IP地址。

   通过查看*tacsplog*日志文件，确认执行结果是否成功。

10.7.6. 调用加密实例

10.7.6.1. 创建Demo实例

本文介绍如何创建Java的Demo实例。

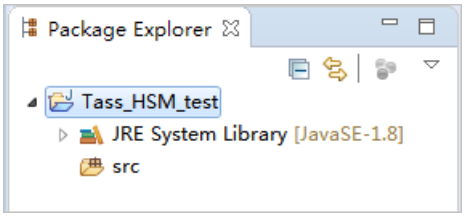
背景信息

VsmManager管理工具和密文通讯方式配置完成后，您就可以通过调用API接口，使用加密服务。

本文创建JAVA的Demo实例后，您可以通过JAVA源文件了解如何调用加解密的API接口，实例说明参见Demo实例说明。

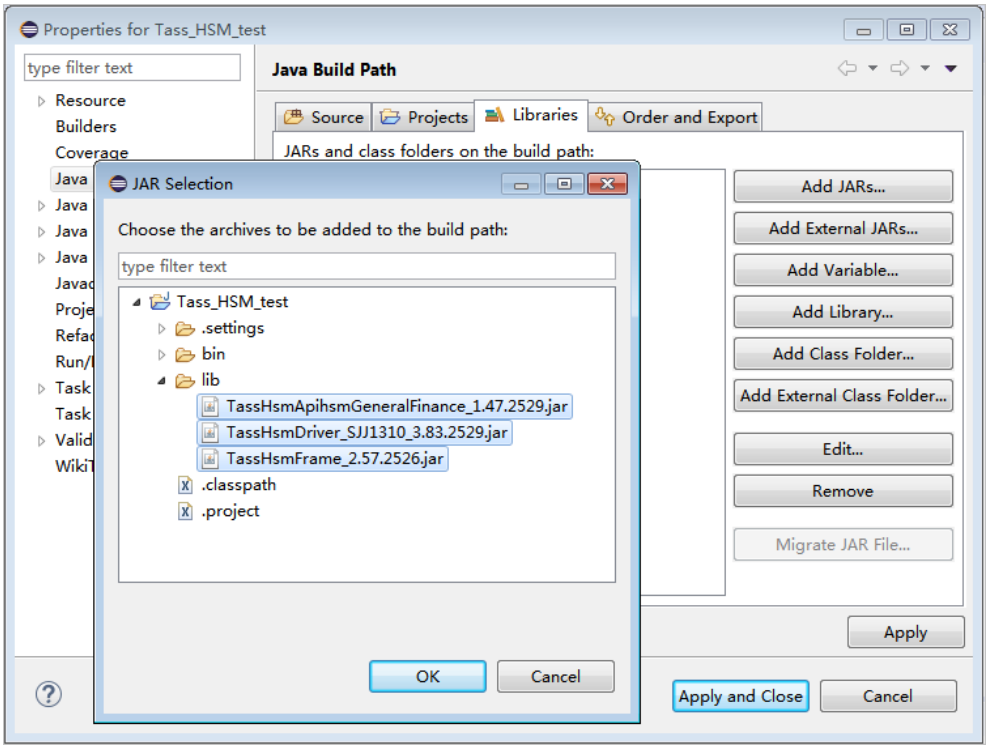
操作步骤

1. 在Eclipse中新建Java工程。
   i. 选择**File > New > Java Project**。
   ii. 在**Project name**中输入工程名称。
   iii. 单击**Finish**。
   创建Java工程实例如下所示。



2. 导入jar包。
   加密服务需要的3个jar包：
   - *TassHsmApihsmGeneralFinance_1.47.2529.jar*
   - *TassHsmDriver_SJJ1310_3.83.2529.jar*
   - *TassHsmFrame_2.57.2526.jar*

   i. 右键单击工程名称，选择**New > Folder**。
   ii. 在**Folder name**中输入*lib*，单击**Finish**。
   iii. 复制*TassHsmApihsmGeneralFinance_1.47.2529.jar*、*TassHsmDriver_SJJ1310_3.83.2529.jar*、*TassHsmFrame_2.57.2526.jar*包。
   iv. 右键单击**lib**，选择**Paste**。
   v. 右键单击工程名称，选择**Build Path > Configure Build Path**。
   vi. 在**Libraries**页签下，单击**Add JARs**。



vii. 选择*lib*中的3个jar包，单击OK。

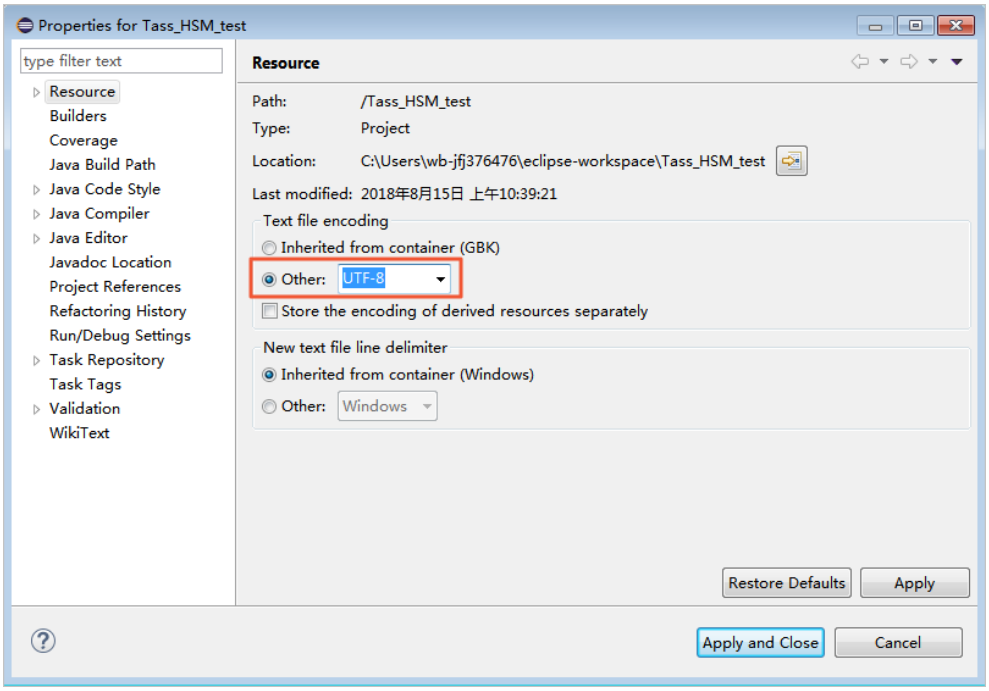
viii. 单击Apply and Close。

3. 修改编码格式为*UTF-8*。

i. 右键单击工程名称，选择Properties。

ii. 单击Resource。

iii. 在Text file encoding中选择Other，并在下拉菜单中选择*UTF-8*。



iv. 单击Apply and Close。

4. 复制Java实例文件到工程中。

Java demo文件：*test_hsmGeneralFinance.java*。

i. 复制*test_hsmGeneralFinance.java*。

ii. 右键单击*src*目录，选择Paste。

10.7.6.2. Demo实例说明

本文介绍Demo实例。

实例化接口

以配置文件形式实例化接口，代码如下：

```
hsmGeneralFinance hgf = hsmGeneralFinance.getInstance("F:\\cacipher.ini");
```

*cacipher.ini*文件说明如下：

```
[LOGGER]
logsw           =       error,info
logPath         =       F://error
[HOST 1]
hsmModel        =       SJJ1310
linkNum         =       1
host            =       192.168.19.132
port            =       8018
timeout         =       15
encodetype      =       0
msgheadlength   =       0
```

配置说明

配置项		说明
[LOGGER]	logsw	输出日志的类型。
	logPath	输出日志的路径。
[HOST 1]	hsmModel	密码机型号：*SJJ1310*。
	linkNum	连接数，取值范围：1~64。
	host	密码机的IP。
	port	端口，固定为8018端口。
	timeout	设置为默认值。
	encodetype	设置为默认值。
	msgheadlength	设置为默认值。

对称加解密

对称加解密代码如下：

```
int algType = 0;
        String keyType = "00A";
        int symmKey = 1;
        String disperFactor = null;
        int sessionType = 0;
        String sessionFactor = null;
        int padFlag = 1;
        byte [] inData = mm.getBytes();
        String IV = "1111111111111111";
        byte [] symmEnc = hgf.generalDataEnc(algType, keyType, symmKey, disperFactor, sessi
onType, sessionFactor, padFlag, inData, IV);
        System.out.println("16进制字符串输出对称加密结果"+Forms.byteToHexString(symmEnc));
        byte [] symmDec = hgf.generalDataDec(algType, keyType, symmKey, disperFactor, sessi
onType, sessionFactor, padFlag, symmEnc, IV);
        System.out.println("字符串输出解密结果"+new String (symmDec));
```

- 对称加密API为generalDataEnc，具体说明参见*云盾API*中的generalDataEnc章节。
- 对称解密API为generalDataDec，具体说明参见*云盾API*中的generalDataDec章节。

RSA非对称加解密

RSA非对称加密代码如下：

```
padFlag = 1;
        byte [] indata = mm.getBytes();
        int RSAkeyPair = 1;
        byte[] RsaPublicKeyEnc = hgf.RsaPublicKeyEnc(padFlag, indata, RSAkeyPair);
        System.out.println("16进制字符串输出RSA公钥解密结果"+Forms.byteToHexString(RsaPublicKe
yEnc));
        byte[] RsaPrivateKeyDec = hgf.RsaPrivateKeyDec(padFlag, RSAkeyPair, RsaPublicKeyEnc
);
        System.out.println("输出RSA私钥解密结果"+new String(RsaPrivateKeyDec));
```

- RSA非对称加密API为RsaPublicKeyEnc，具体说明请参见*云盾API*中的RsaPublicKeyEnc章节。
- RSA非对称解密API为RsaPrivateKeyDec，具体说明请参见*云盾API*中的RsaPrivateKeyDec章节。

10.8. 堡垒机

10.8.1. 概述

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。

云盾堡垒机基于账号（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。

10.8.2. 快速部署指南

10.8.2.1. 部署堡垒机系统

该章节介绍如何部署堡垒机系统。

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。

背景信息

堡垒机系统通过镜像方式部署在专有云的服务器中。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**运维审计 > 租户堡垒机**。
3. 单击**我要创建**，进入**云服务器ECS**页面。

4. 选择**实例**页签，单击**创建实例**。
5. 在**创建云服务器ECS**页面，创建云盾堡垒机系统服务器。
   i. 设置区域、配置基本配置、网络等信息。
   ii. 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：8 G

   iii. 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。
   iv. 配置40 G的系统盘和800 G的数据盘。

   > **说明** 数据盘至少需要100 G，否则服务无法启动。

   v. 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。
6. 联系销售人员，申请云盾堡垒机系统正式版的License许可。

10.8.2.2. 配置自定义IP

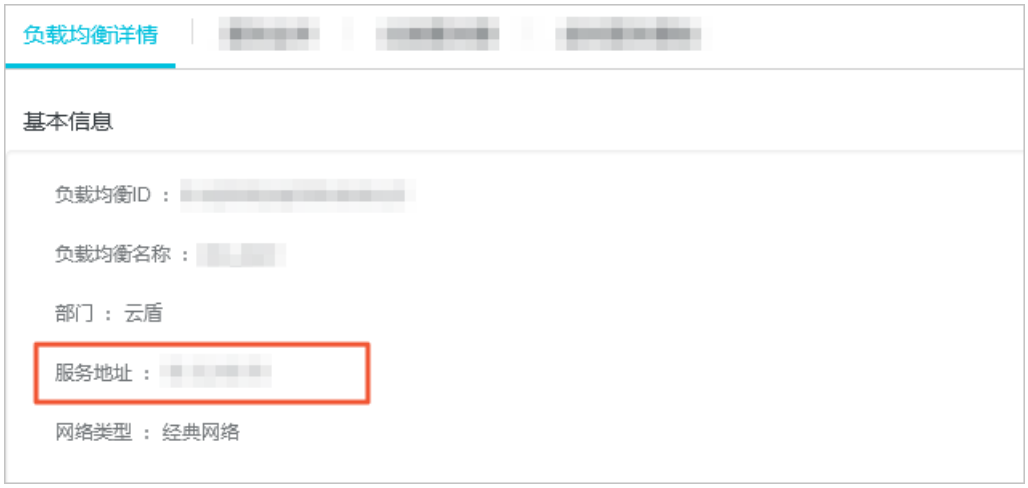
本文介绍如何配置堡垒机的自定义IP。

背景信息

云盾用户通过自定义IP，可以在云盾安全中心直接访问堡垒机。

操作步骤

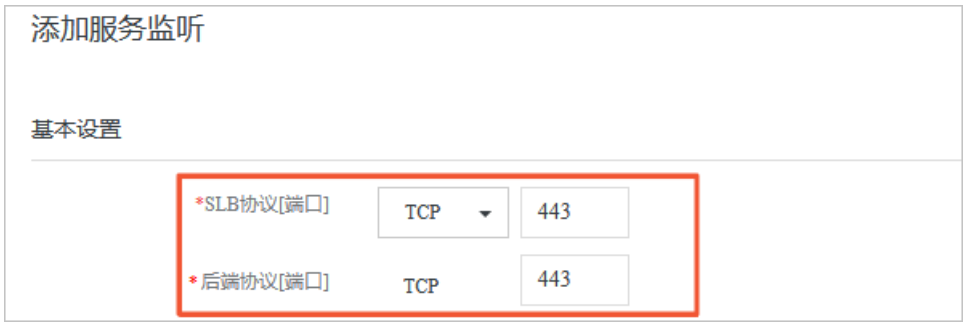
1. 登录Apsara Uni-manager运营控制台。
   具体步骤，请参见登录云盾安全中心的步骤1到步骤4。
2. 创建堡垒机的SLB服务。
   具体操作，请参见*负载均衡用户指南*的**创建负载均衡实例**章节，创建负载均衡实例。创建完成后，进入负载均衡实例，记录下SLB的服务地址。



> **说明** SLB的服务地址就是堡垒机的自定义IP。

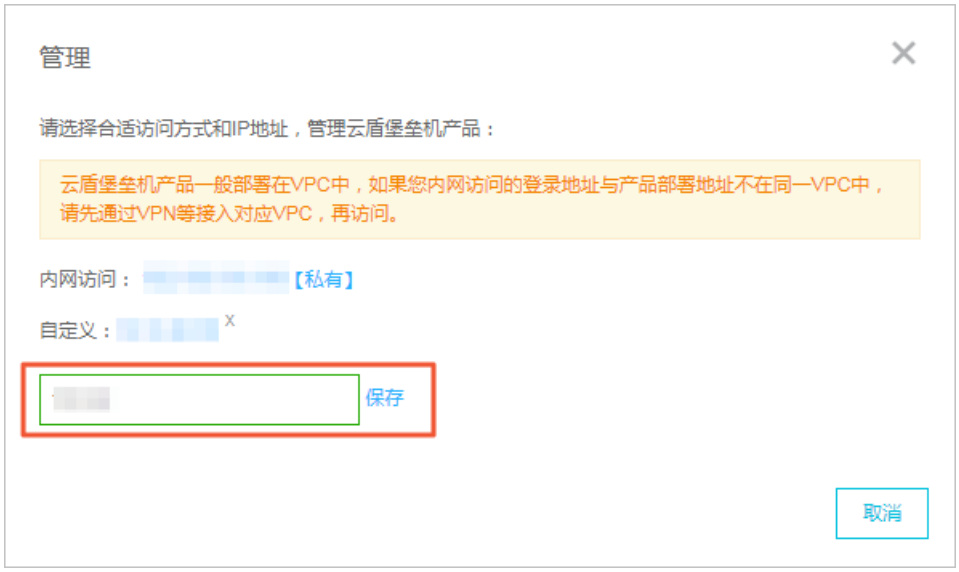
其中，SLB的**服务监听**和**后端服务器**配置如下：

- **服务监听**：设置TCP协议和443端口，如下图所示。



- **后端服务器**：选择堡垒机的服务器。

3. 登录云盾安全中心。
4. 在控制台右上方，单击**安全**，选择**运维审计 > 租户堡垒机**。
5. 在云盾堡垒机的**操作**栏，单击**管理**。
6. 在**管理**对话框中，单击**新增自定义访问地址**。
7. 输入SLB的服务地址，单击**保存**。



10.8.2.3. 登录云盾堡垒机（云盾安全中心登录）

本章节介绍如何在云盾安全中心上使用admin超级管理员直接登录云盾堡垒机。

背景信息

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。

首次登录堡垒机后，需要修改admin用户的默认密码，请从技术支持人员处获取。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**运维审计 > 租户堡垒机**。

3. 在需要登录云盾堡垒机的**操作**栏，单击**管理**，查看登录信息。
4. 单击**自定义**后面的IP地址，登录到云盾堡垒机。
5. 在默认的**个人信息**页面，分别输入旧密码和新密码，单击**保存更改**。

> **说明** 如果部署堡垒机后，第一次登录堡垒机，需要参照该步骤修改默认密码。修改之后再次登录堡垒机，将不需要执行此步骤。

10.8.2.4. 登录云盾堡垒机（一般Web方式登录）

本章节介绍如何登录云盾堡垒机。

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相应的用户名和密码，云盾堡垒机的基本角色如下表所示。

用户	说明
超级管理员	超级管理员账号：admin **说明** admin用户必须从云盾安全中心登录，具体参考登录云盾堡垒机（云盾安全中心登录）。
审计管理员	审计人员通过此账号进行审计，由超级管理员在**用户管理**中创建。
系统管理员	系统管理员通过此账号进行系统管理，由超级管理员在**用户管理**中创建。
运维员	运维人员通过此账号维护主机，由超级管理员在**用户管理**中创建。

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https://*云盾堡垒机系统IP地址*，按回车键（Enter）。

   云盾堡垒机系统登录页面



3. 输入正确的用户名、密码及验证码。

   用户由超级管理员在**用户管理**中创建。

4. 单击**登录**，进入云盾堡垒机系统。

> **说明** 首次登录成功后，管理员必须修改密码。

10.8.2.5. 导入许可证

该章节介绍如何导入堡垒机的许可证。

背景信息

堡垒机需要导入许可证才能正常使用。如果您初始导入许可证或到期更换许可证，可以参考本章节内容操作。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 许可证**页面。



3. 申请许可证。
   i. 单击**生成系统认证文件**。
   ii. 将系统认证文件导出后，与相关人员联系并获取许可证文件。
4. 备份许可证。

   获取到有效的许可证文件之后，可将原有的许可证带出到本地备份保存。如果首次导入许可证，可以忽略此步骤。
   i. 单击**备份许可证**。
   ii. 选择本地路径并保存。
5. 导入许可证。

   获取到有效的许可证之后需要将许可证导入系统生效。
   i. 单击**导入许可证**。
   ii. 选择许可证文件并导入。

10.8.3. 超级管理员快速配置指南

10.8.3.1. 用户管理

10.8.3.1.1. 手工新建用户

本章节介绍如何手工新建云盾堡垒机的用户。

背景信息

通过超级管理员账号为不同用户创建账号并选择适合的角色，各角色所拥有的权限说明如下。

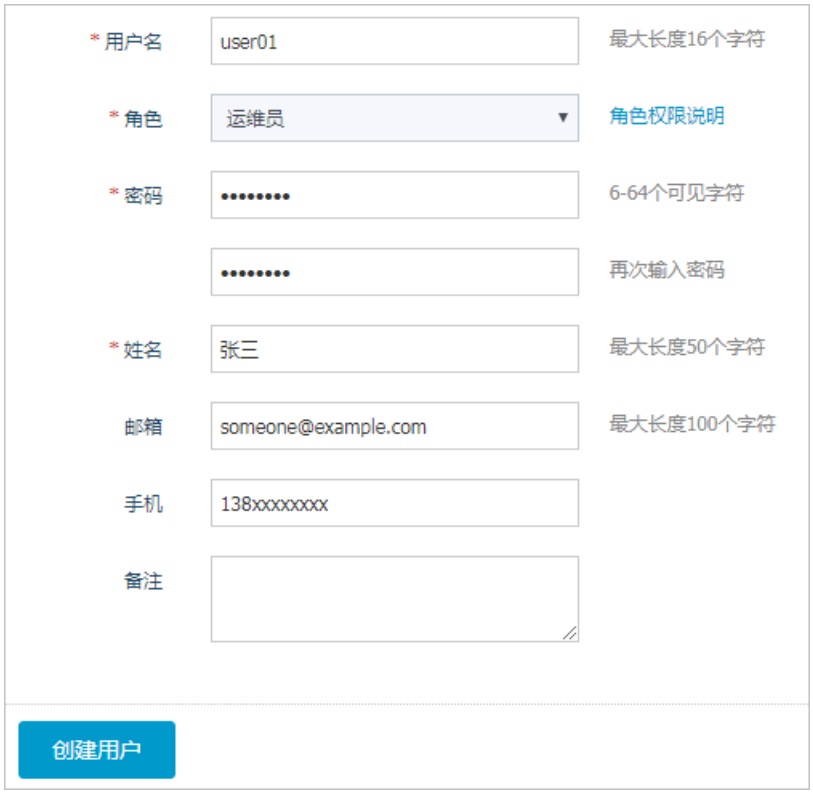
角色权限说明

	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
用户管理 用户增加、删除、编辑	●	●	●	●			
用户组管理 用户组增加、删除、编辑	●	●	●				
资产管理 管理资产	●	●	●				
授权管理 管理运维规则，审批工单	●	●	●				
会话审计 查看、播放、下载历史会话	●	●		●		◑ 需要审计规则允许	
审计规则 管理审计规则	●	●		●			
主机运维 主机运维、应用运维、创建工单、查看运维报表	●	●	●	●	●	●	●
实时监控 管理、审批在线会话	●	●	●				
系统管理 系统配置、操作日志、系统报表、数据维护、系统维护	●						●

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。
3. 单击**新建用户**。
4. 在**新建用户**页面，输入用户信息。

   新建用户



> **说明** 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。

5. 单击**创建用户**。
   创建用户成功，系统提示用户已创建。

10.8.3.1.2. 批量导入用户

本章节介绍如何批量导入云盾堡垒机的用户。

背景信息

如果需要创建的用户数量比较多，可以通过标准模板设置用户信息，再批量导入到云盾堡垒机中。

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。
3. 单击**更多操作**，选择**导入用户**。
4. 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。



5. 根据模板规范要求，制作需要导入的用户列表。

   在模板中需要配置信息如下所示。



# 用户名必填，认证模式为本地认证时密码也必填，其他字段可以不填，样例数据如下所示：					
#用户名	密码	角色	姓名	邮箱	手机
[redacted]	[redacted]	审计员	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	运维员	[redacted]	[redacted]	[redacted]

> **说明** 导入模板由系统提供，不允许自行添加和修改字段，支持*.csv*、*.xls*和*.xlsx*三种格式。

6. 单击**上传文件**，从本地选择制作好的用户列表文件。
7. 在**认证模式**中选择用户登录的认证模式，勾选覆盖已有同名用户。

   认证模式支持*本地认证*、*AD*、*LADP*和*Radius*等方式。

   - *本地认证*：通过本地用户名和密码进行登录认证。
   - *AD*：通过AD服务器进行登录认证。

- *LADP*：通过LADP服务器进行登录认证。
- *Radius*：通过RADIUS服务器进行登录认证。

> **说明** 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。

10.8.3.1.3. 管理用户

该章节介绍如何管理已有用户，包括导出用户、删除用户、锁定用户等操作。

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。
3. 在用户列表中，管理已经创建的用户。
   - 搜索用户

     在搜索框中输入用户名关键字，按Enter键，快速搜索定位用户。

     也可通过用户角色和认证方式进行过滤。
   - 编辑用户
     a. 单击用户名。
     b. 在**基本信息**页面，修改用户信息。
     c. 单击**保存**。
   - 导出用户

     单击右下角的**导出用户**，可以导出并查看用户表信息。
   - 删除用户

     勾选用户，单击**删除**。
   - 锁定用户

     勾选用户，单击**锁定**。

     > **说明** 锁定的用户将不能登录堡垒机，直到管理员解锁为止。
   - 解锁用户

     勾选已锁定用户，单击**解锁**。

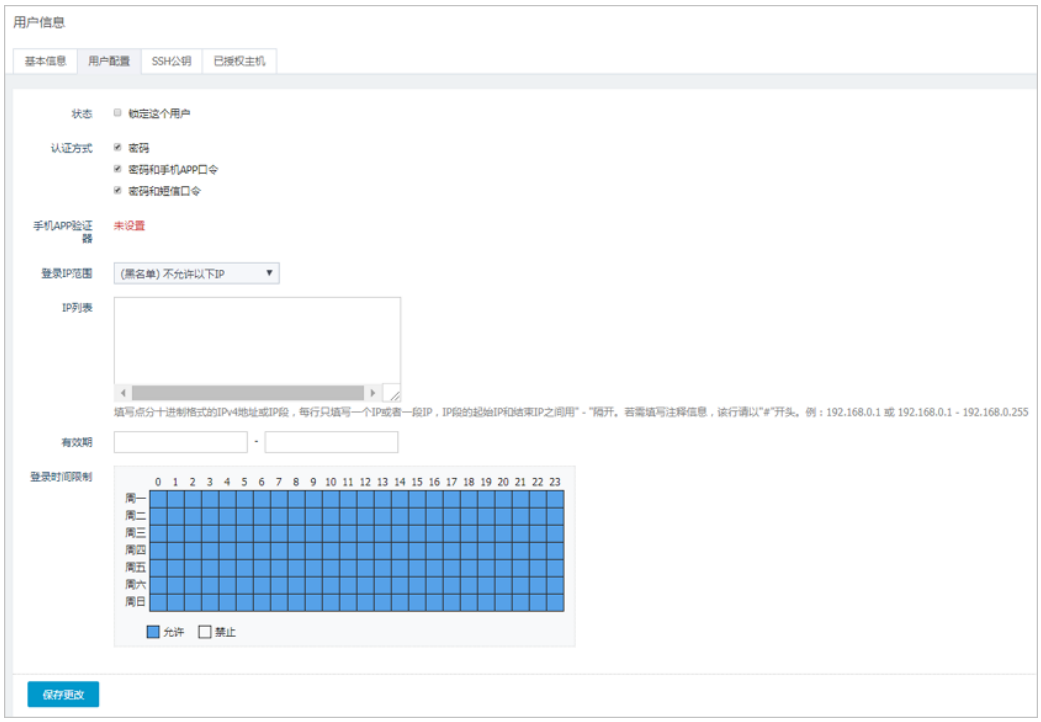
10.8.3.1.4. 配置用户信息

用户创建成功后，管理人员可以进行用户配置、设置SSH公钥和设置已授权主机等操作。

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。

3. 在用户列表中，单击用户名。
4. 在**用户信息**页面，选择**用户配置**页签，设置用户配置并单击**保存更改**。



设置项	说明
状态	锁定、解锁该用户。
认证方式	用户登录时的认证方式，支持密码、密码和手机APP口令、密码和短信口令。
登录IP范围	限制该用户的登录IP范围。
有效期	用户登录有效期。
登录时间限制	限制该用户的登录时间范围。

5. 选择**已授权主机**，可以查看已授权给该用户的所有主机。
6. 选择**SSH公钥**页签，设置用户的公钥。

   SSH公钥用于用户使用SSH协议登录堡垒机系统。

   > **说明** 在设置前，用户需要通过OpenSSH工具生成SSH的公钥和私钥，其中公钥保存到堡垒机中，私钥导入到本地的SSH工具。

   i. 单击**添加SSH公钥**。
   ii. 添加公钥名称和公钥内容。
   iii. 单击**保存**。
7. 设置SSH私钥。

   SSH私钥用于使用SSH协议登录主机。

> **说明** 在设置前，用户需要通过OpenSSH工具生成SSH的公钥和私钥，其中私钥保存到堡垒机中，公钥保存到目标主机。

i. 单击右上角的**个人信息 > SSH私钥**。
ii. 输入SSH私钥信息。
iii. 单击**保存私钥**。

10.8.3.2. 用户组管理

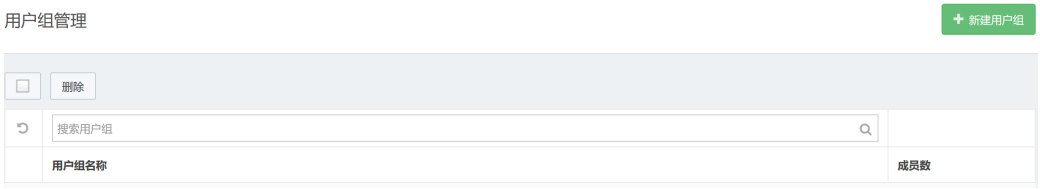
10.8.3.2.1. 新建用户组

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

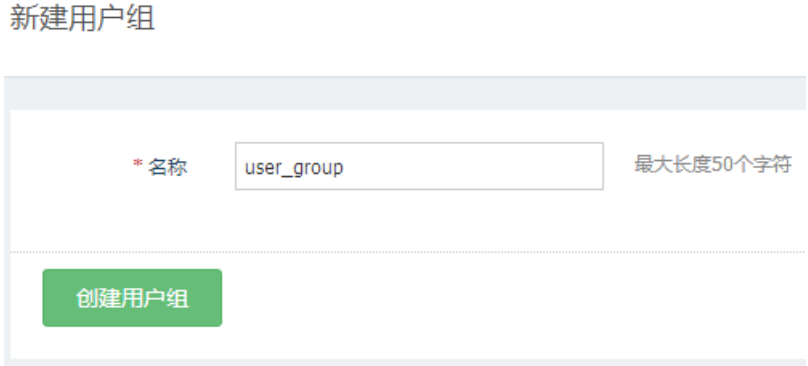
1. 使用超级管理员（admin）账号登录云盾堡垒机系统。
2. 定位到**用户 > 用户组管理** 页面，如用户组管理页面所示。

   用户组管理页面



3. 单击**新建用户组**。
4. 填写用户组名称，单击**创建用户组**，如新建用户组所示。

   新建用户组



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。

10.8.3.2.2. 管理用户组

该章节介绍如何对用户组进行搜索、修改、删除等操作。

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. 在用户组列表中，管理用户组。
   - 搜索用户组

     在搜索框中输入用户组关键字，按Enter键，快速搜索定位用户组。
   - 修改用户组信息
     a. 直接单击用户组名称。
     b. 在**用户组信息**页面，单击**修改用户组名称**。
     c. 输入新的用户组名。
     d. 单击**保存更改**。
   - 删除用户组
     a. 勾选需要删除的用户组。
     b. 单击**删除**。

10.8.3.2.3. 对用户进行分组

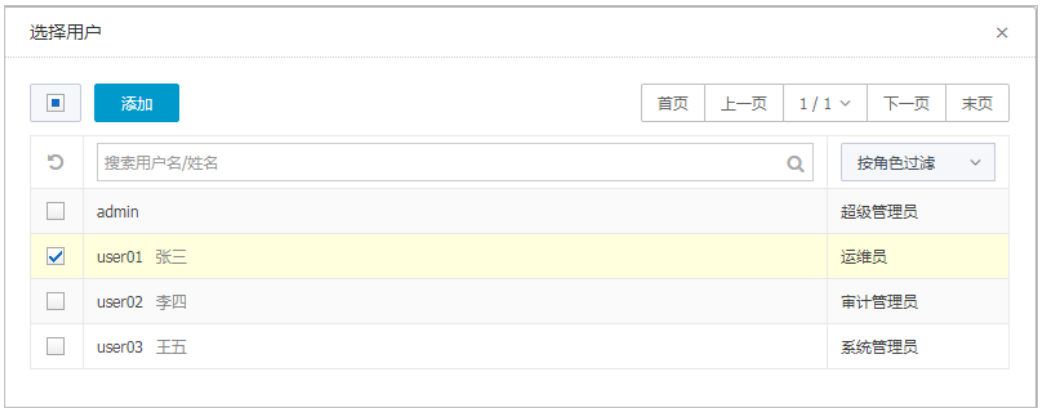
根据用户的业务需要，分配到不同的用户组。

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。
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**，如选择用户所示。

   > **说明** 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。

   选择用户

   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。

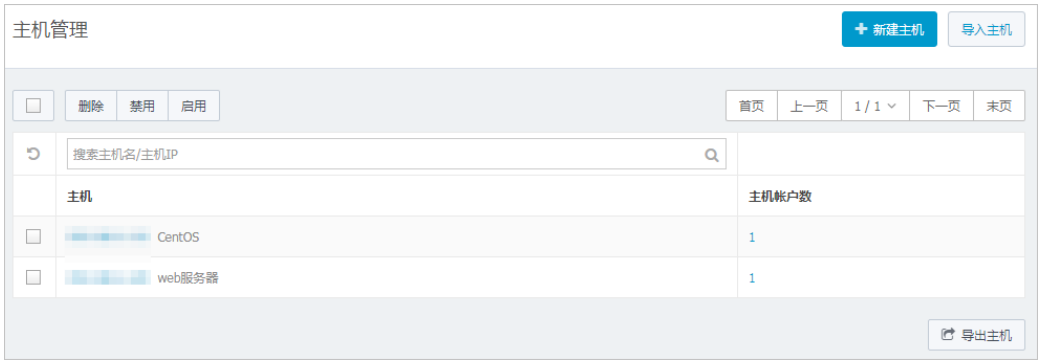
10.8.3.3. 主机管理

10.8.3.3.1. 手工新建主机

手工关联需要通过堡垒机进行维护的服务器。

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**新建主机**。
4. 在**新建主机**页面，设置**主机IP**和**主机名称**等信息。



> **说明** 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。

10.8.3.3.2. 批量导入主机

批量导入需要通过堡垒机进行维护的服务器。

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**。
4. 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，如导入主机页面所示。

   导入主机页面



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。

   > **说明** 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。

10.8.3.3.3. 管理主机信息

该章节介绍如何管理主机信息，包括修改主机信息、删除主机等操作。

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. 在主机列表中，管理主机。
   - 搜索主机

     在搜索框中输入主机IP/主机名，按Enter键，快速搜索主机。
   - 导出主机信息

     单击右下角的**导出主机**即可完成导出。

     导出的信息包括主机IP、主机名称、操作系统、主机帐户登录名、帐户密码、协议:端口、主机组、主机网络。此文件可直接导入堡垒机，故可以通过此方式对主机和主机帐户进行批量修改。
   - 删除主机

勾选主机，单击**删除**。

- 禁用主机

  勾选主机，单击**禁用**。

  用户不能访问被禁用的主机。

- 启用主机

  勾选被禁用主机，单击**启用**。

- 修改主机基本信息

  a. 单击主机对应的IP地址。

  b. 在**主机信息**页面，选择**基本信息**页签。

  c. 修改主机IP、主机名称、协议端口号等信息。

  > **说明** 此处协议端口指的是目标主机上，该协议对应的端口号。如果用户的主机出于安全考虑不用默认端口号时，需要在此处将协议端口号设置为真实的端口。

  d. 单击**保存更改**。

10.8.3.3.4. 设置主机帐户

该章节介绍如何设置目标主机的帐户。

背景信息

主机帐户是用于登录目标主机及应用的管理帐户，堡垒机支持7种协议的帐户：SSH、TELNET、FTP、SFTP、RDP、VNC、Rlogin。

> **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。

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. 在**主机管理**页面的主机列表中，单击已添加的主机IP。
4. 选择**主机帐户**页签，单击**添加主机帐户**。



5. 在**新建主机帐户**对话框中，设置主机帐户信息。



6. 单击**验证**，验证主机帐户和密码是否正确。
7. 验证成功后，单击**创建主机帐户**。

后续步骤

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。

10.8.3.3.5. 管理主机配置

主机添加成功后，管理人员可以对主机进行相关配置。

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**，如更改主机配置信息所示。

   更改主机配置信息



10.8.3.4. 主机组管理

10.8.3.4.1. 新建主机组

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。

   主机组管理页面



3. 单击**新建主机组**，进入**新建主机组**页面，如新建主机组页面所示。

   新建主机组页面



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。

10.8.3.4.2. 管理主机组

该章节介绍如何管理主机组，包括搜索、修改、删除等操作。

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。
3. 在**主机组管理**页面，管理主机组。
   - 搜索主机组

     在主机组列表搜索框中，输入主机组关键字，按Enter键。
   - 修改主机组名称
     a. 在主机组列表中，直接单击主机组名称。
     b. 选择**修改主机组名称**页签，修改主机组名称。
     c. 单击**修改保存**。
   - 删除主机组

     在主机组列表中，勾选主机组，单击删除。

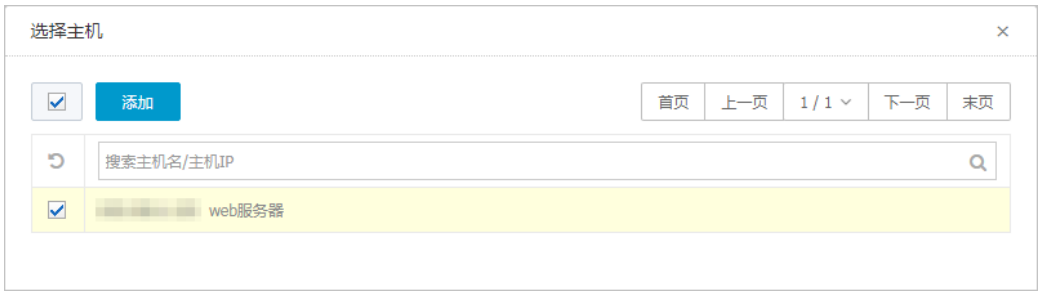
10.8.3.4.3. 对主机进行分组

主机根据各自的业务需要，分配到不同的主机组。

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。
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**，如选择主机所示。

   选择主机

   说明 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。

10.8.3.5. 帐户组管理

10.8.3.5.1. 新建帐户组

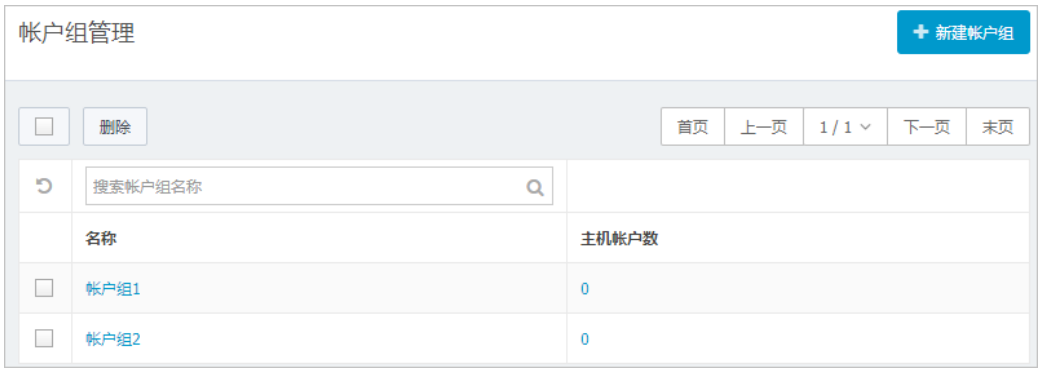
该章节介绍如何新建帐户组。

背景信息

帐户组用于对主机帐户的分组，方便在授权的时候进行帐户的批量授权。

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 > 帐户管理**页面。

3. 单击**新建帐户组**。

4. 在配置页面，设置帐户组信息。
5. 单击**创建帐户组**，完成账户组的创建。

10.8.3.5.2. 管理帐户组信息

该章节介绍如何管理帐户组，包括搜索账户组、编辑账号组信息、删除账户组等。

背景信息

当运维的网络环境发生变化时，帐户组可能也需要根据变化进行调整，用于适应网络环境。

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 > 帐户管理**页面。
3. 在**帐户组管理**页面，管理帐户组。
   - 搜索帐户组

     在帐户组列表的搜索框，输入帐户组关键字，按Enter键。
   - 编辑帐户组信息
     a. 在帐户组列表中，直接单击帐户组名称。
     b. 选择**主机帐户**页签，添加或删除帐户组成员。
     c. 选择**修改帐户组名称**页签，编辑帐户组名称。
   - 删除帐户组

     在帐户组列表中，勾选帐户组，单击**删除**。

10.8.3.6. 运维授权

10.8.3.6.1. 运维规则概述

该章节介绍运维规则的主要关系类型。

运维规则是将堡垒机中的用户与主机资产联系在一起的概念，通过授权运维规则功能可以达到控制某个用户只能访问他权限内主机的目的。

运维规则关系类型主要包括：

- 帐户组授权给用户组
- 单个主机帐户授权给用户组
- 主机组授权给用户组
- 帐户组授权给单个用户
- 单个主机帐户授权给单个用户
- 主机组授权给单个用户

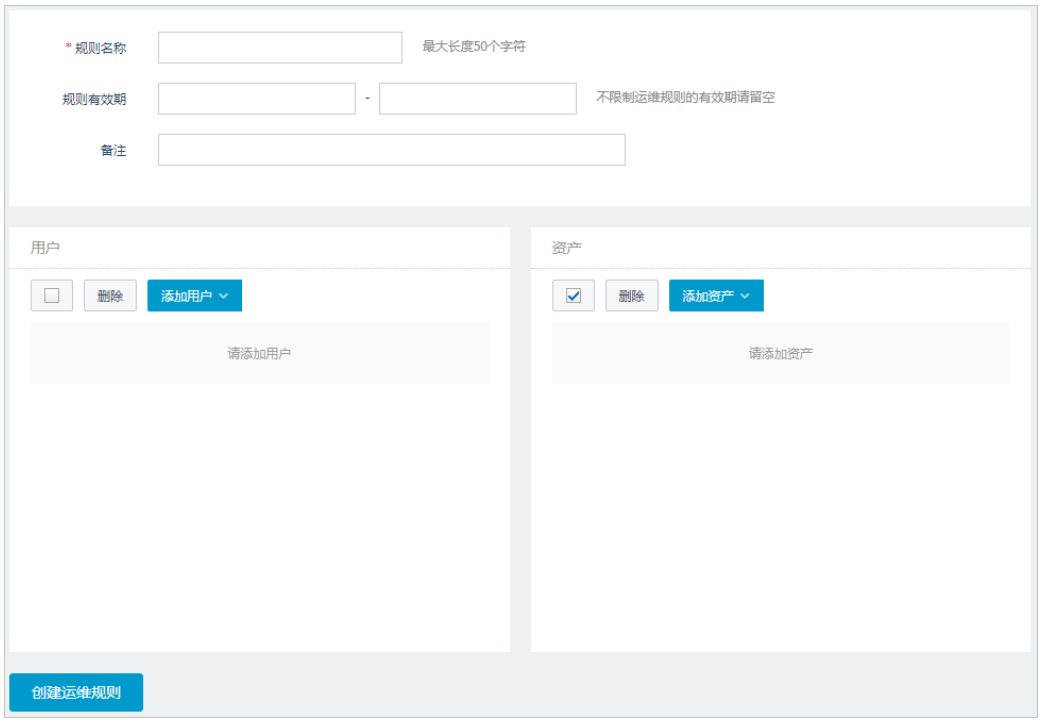
10.8.3.6.2. 新建运维规则

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。

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**授权 > 运维规则** 页面。
3. 单击**新建运维规则**。

   新建运维规则页面

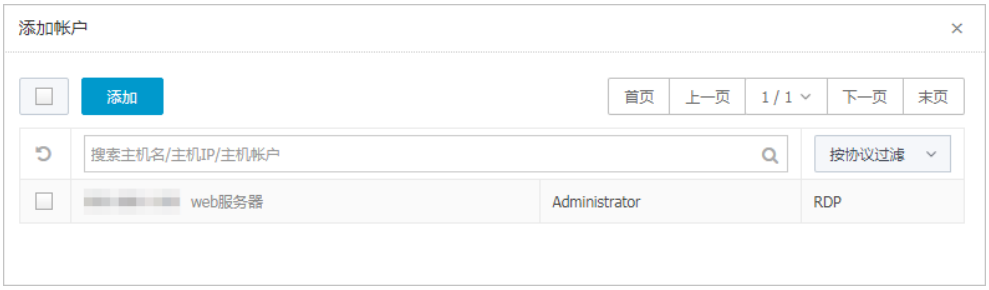


4. 在**新建运维规则**页面，设置**规则名称**、**规则有效期**等规则基本信息。
5. 在**新建运维规则**页面，添加运维用户。
   i. 单击**添加用户**，选择**添加用户**或**添加用户组**。
   ii. 勾选需要授权的用户或用户组，单击**添加**。



6. 在**新建运维规则**页面，添加运维资产。
   i. 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**。

ii. 勾选需要授权的主机帐户、帐户组或者主机组，单击**添加**。



7. 在**新建运维规则**页面，单击**创建运维规则**。

10.8.3.6.3. 管理运维规则

运维规则创建后，管理人员可以对运维规则进行相关配置。

操作步骤

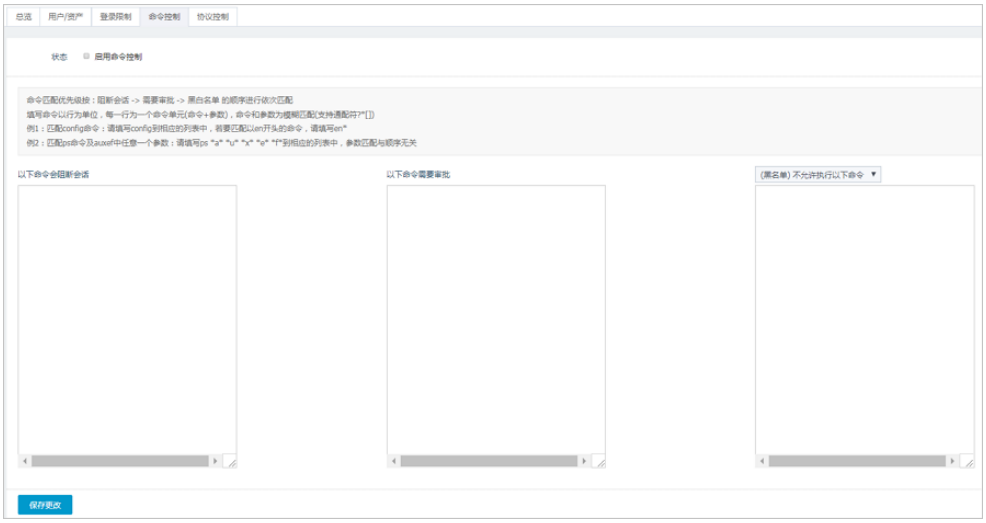
1. 使用超级管理员（admin）账号登录云盾堡垒机系统。
2. 定位到**授权 > 运维规则** 页面。
3. 选择已添加的运维规则，执行相关操作。
   - 编辑运维规则

     在运维规则列表中，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。



- 在**命令控制**页签，可以启用命令控制、命令阻断，命令审批和命令黑白名单功能。



- 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。



> **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。

- 禁用规则

  在运维规则列表中，勾选运维规则，单击**禁用**。

- 启用规则

  在运维规则列表中，勾选已禁用运维规则，单击**启用**。

- 删除规则

  在运维规则列表中，勾选运维规则，单击**删除**。

- 复制规则

  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。

10.8.3.7. 未授权运维审核

10.8.3.7.1. 未授权登录审核

该章节介绍如何对未授权的登录行为进行审核。

前提条件

在**系统 > 系统配置 > 运维配置**页面中，已设置**收集未授权登录**。

背景信息

如果用户和主机不在运维规则中，当用户要登录该主机时，会生成一条未授权登录的审核条目。管理员审核通过后，用户才能登录该主机，同时系统会自动创建一条该用户和主机的运维规则。

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**授权 > 未授权登录审核**页面。
3. 勾选需要进行授权的条目，单击**授权**进行授权。
4. （可选）管理未授权审核条目。
   - 搜索审核条目

     输入主机名、用户名或主机账户进行模糊搜索，也可以根据协议和授权状态进行过滤。
   - 删除审核条目

     勾选需要删除的条目，单击**删除**。

10.8.3.7.2. 审批运维工单

该章节介绍管理员如何审批运维人员申请的工单。

前提条件

运维人员已经申请工单，具体参见新建工单。

背景信息

当运维人员需要运维授权关系以外的主机，且管理员并没有开启未授权登录时，运维人员可以通过工单向管理员申请运维这些资产。管理员批准工单后系统将自动创建工单中的授权关系。

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**工单 > 工单审批**页面。
3. 根据实际需求审批工单。
   - 修改工单

     工单处于待审批状态，单击工单号或工单后的**详情**对运维员申请的工单进行修改。
   - 批准工单

     勾选工单申请条目，单击**批准**。

- 拒绝工单

  勾选工单申请条目，单击**拒绝**。

10.8.3.8. 实时监控

该章节介绍管理员如何对运维过程实时监控。

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。如果运维人员有不当操作，管理员可以直接阻断会话。

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，管理实时会话。



- 查看详情

  单击操作栏中的**详情**，可查看详细的会话信息。

- 播放会话

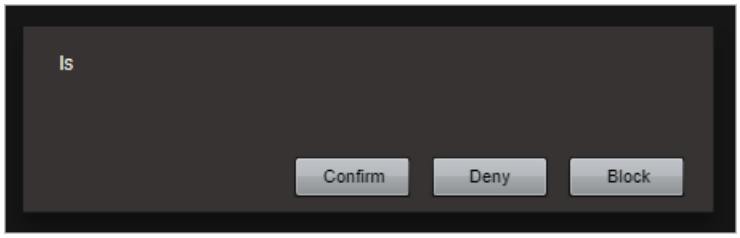
  单击操作栏中的**播放**，可通过Web方式查看会话实时回放。

  > **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。

- 阻断会话

  如果运维人员的操作属于高危操作，管理员通过单击**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。

4. 选择**需要命令审批**页签，管理命令审批。
   i. 单击会话条目右侧的**播放**。
   ii. 在**运维窗口监控**页面，实时查看运维会话的操作情况。
   iii. 在弹出的命令审批对话框中，根据实际情况审批命令。



10.8.4. 运维人员操作指南

10.8.4.1. 下载运维工具

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. 使用运维员账号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，如工具下载页面所示。

   工具下载页面



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。

   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。

运维工具	说明
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，进行离线播放的工具。
Adobe ATR	
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。

10.8.4.2. Web方式运维（适用于Windows）

10.8.4.2.1. 安装单点登录器

该章节介绍如何安装单点登录器。

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。

> **说明** 仅适用于使用Windows客户端的运维人员。

操作步骤

1. 使用运维员账号登录云盾堡垒机系统。
2. 下载单点登录器安装程序。

   下载方式请参考下载运维工具。
3. 在本地PC上，双击单点登录器安装程序。
4. 选择安装语言，单击**OK**。
5. 在**选定安装位置**中，设置安装目标文件夹，单击**安装**。
6. 安装成功后，在安装成功提示框中，单击**确定**。

10.8.4.2.2. 指定运维工具

该章节介绍如何指定各协议的运维工具。

背景信息

本章节以指定PuTTY工具为SSH协议登录方式为例进行介绍。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. 使用运维员账号登录云盾堡垒机系统。
2. 定位到**运维 > 主机运维**页面。
3. 单击右上角的**Web运维配置**。
4. 在**Web运维配置**对话框中，选择登录协议。

   本章节以SSH为例，此处选择**SSH & TELNET & Rlogin**。
5. 在**客户端程序**中，选择*PuTTY*。

   > **说明** 您也可以选择其他SSH运维工具，在选择前，您需要确认已安装了所选择的客户端程序。
6. 单击**保存**。

   > **说明** 如果浏览器弹出要打开URL：USM Single-On吗？的提示，请单击**打开URL：USM Single Sign-On**。
7. 在**单点登录配置**对话框中，设置客户端。



   i. 单击**浏览**。
   ii. 选择客户端程序所在的位置，单击**打开**。
   iii. 单击**确定**。

10.8.4.2.3. 通过SSH协议登录主机进行运维

该章节介绍如何以SSH协议对目标主机进行运维。

操作步骤

1. 使用运维员账号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**。

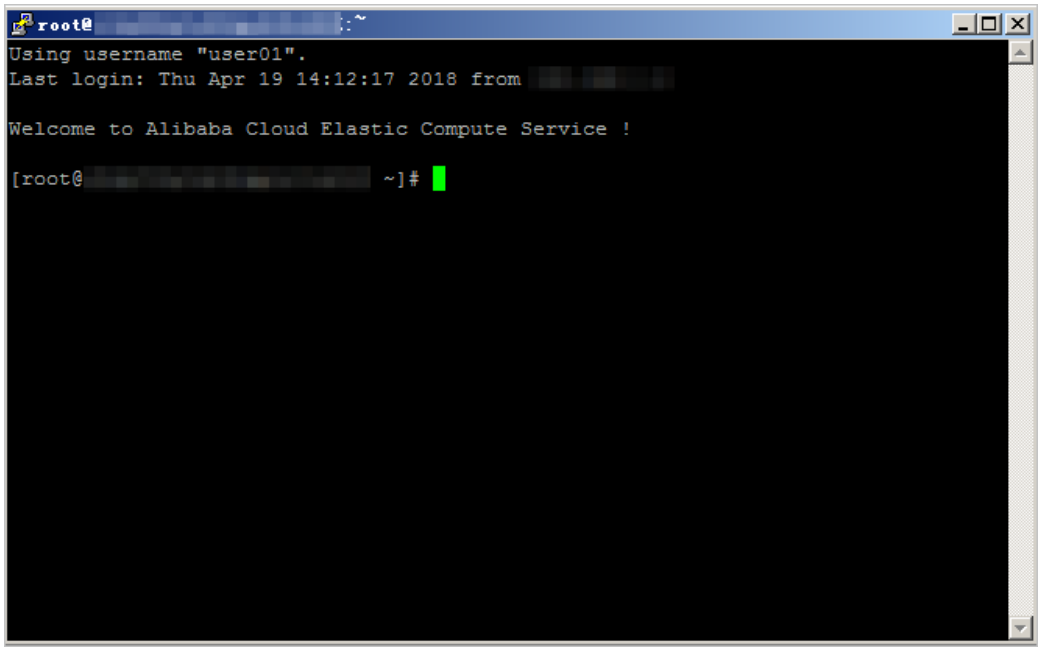
> **说明** 如果浏览器弹出要打开URL：USM Single-On吗？的提示，单击**打开URL：USM Single Sign-On**。

SSH协议主机Web运维



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。

SSH协议主机运维操作



> **说明** 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。

10.8.4.2.4. 通过RDP协议登录主机进行运维

该章节介绍如何以RDP协议对目标主机进行运维。

操作步骤

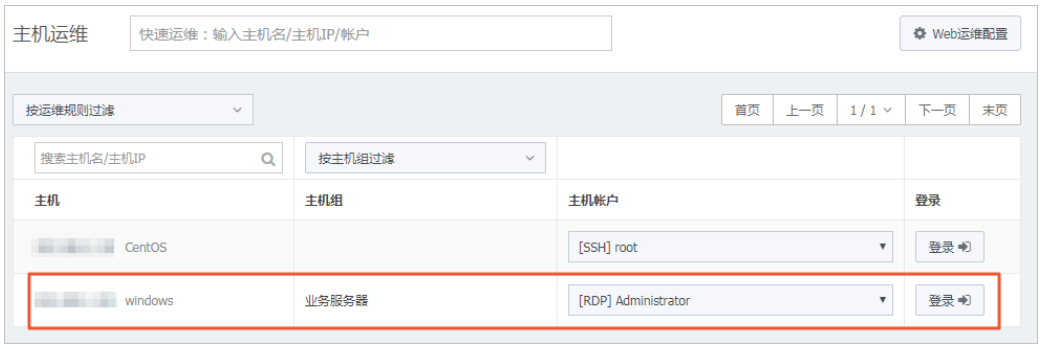
1. 使用运维员账号登录云盾堡垒机系统。
2. 定位到**运维 > 主机运维** 页面。

> **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RDP协议的主机帐户，单击**登录**。

> **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**。

RDP协议主机Web运维



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。

> **说明** 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。

10.8.4.2.5. 通过SFTP协议登录主机进行运维

该章节介绍如何以SFTP协议对目标主机进行运维。

操作步骤

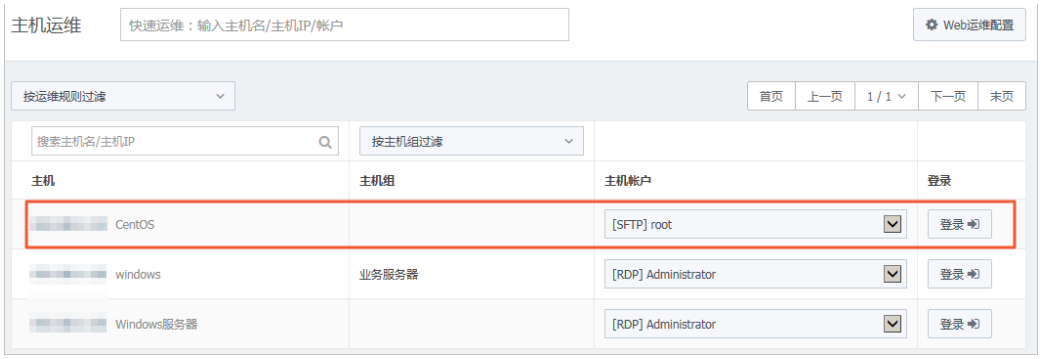
1. 使用运维员账号登录云盾堡垒机系统。
2. 定位到**运维 > 主机运维** 页面。

> **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SFTP协议的主机帐户，单击**登录**。

> **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**。

SFTP协议主机Web运维



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。

> **说明** 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。

10.8.4.2.6. 未授权登录主机进行运维

该章节介绍如何对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

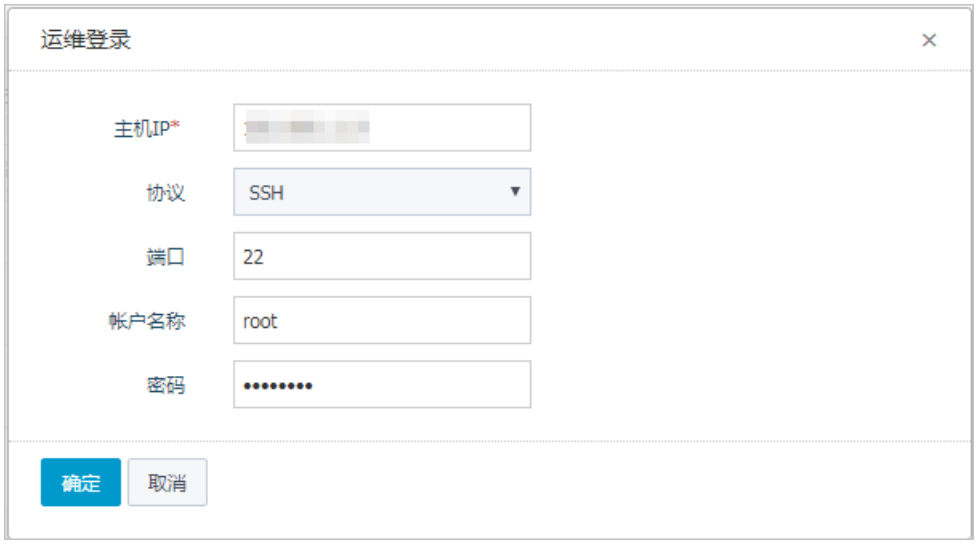
1. 使用运维员账号登录云盾堡垒机系统。
2. 定位到**运维 > 主机运维**页面，单击**未授权登录**。

   未授权登录



3. 在**运维登录**对话框中，输入主机IP等信息。

   未授权运维登录对话框



> **说明** 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。

4. 单击**确定**。

10.8.4.2.7. 运维审批申请

如果开启**开启会话二次审批**，运维人员需要提交运维审批申请。

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. 使用运维员账号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。

> **说明** 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。

10.8.4.3. CS方式运维操作指南

10.8.4.3.1. 在苹果操作系统上运维

10.8.4.3.1.1. 准备工作

该章节介绍在苹果系统上使用云盾堡垒机运维需要的一些准备工作。

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。

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

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。

背景信息

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。

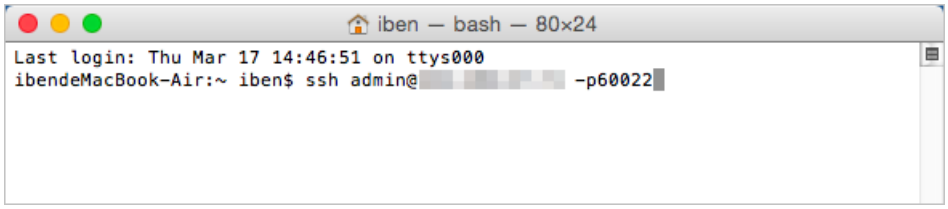
操作步骤

1. 打开命令行终端app，输入以下命令，按回车键（Enter）。

   ```
   ssh 云盾堡垒机系统的用户名@云盾堡垒机系统的IP -p60022
   ```

   - *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。

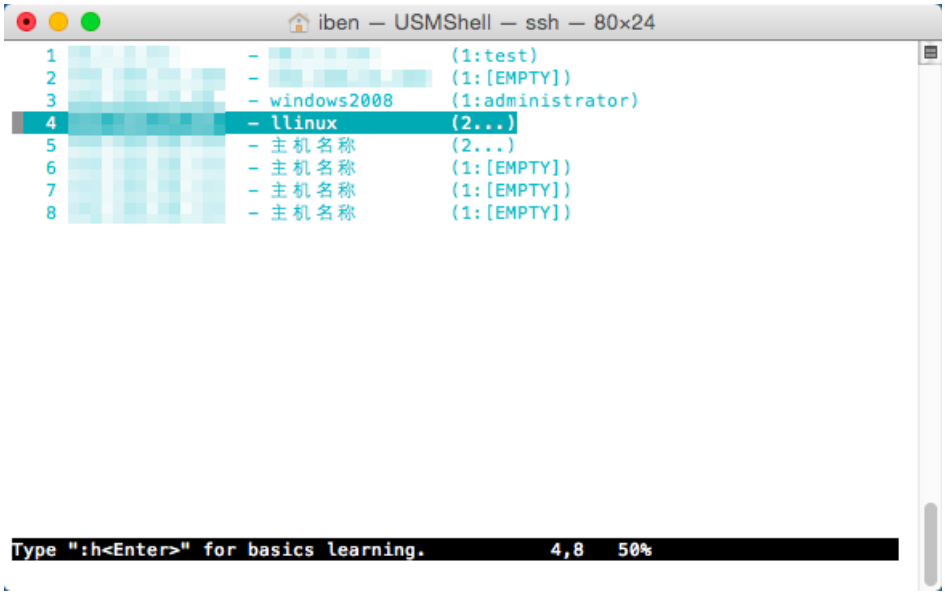
     通过命令行终端登录云盾堡垒机

   > **说明**
   >
   > 如果提示需要输入密码，请输入该用户的密码，按回车键（Enter）。

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）。

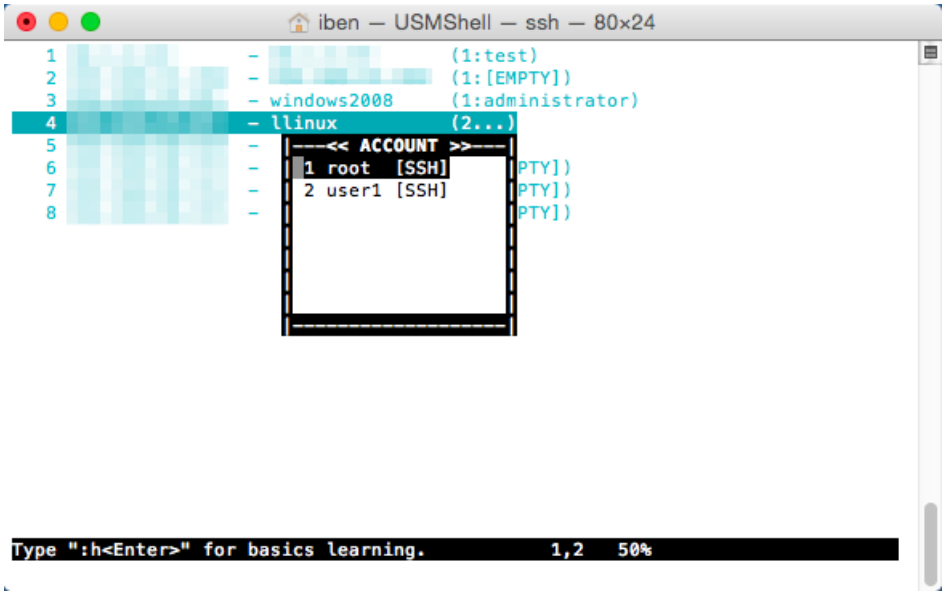
   通过命令行终端选择主机资产



3. 选择主机账户，按回车键（Enter）。

> 说明 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）。

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。

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

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。

背景信息

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**。

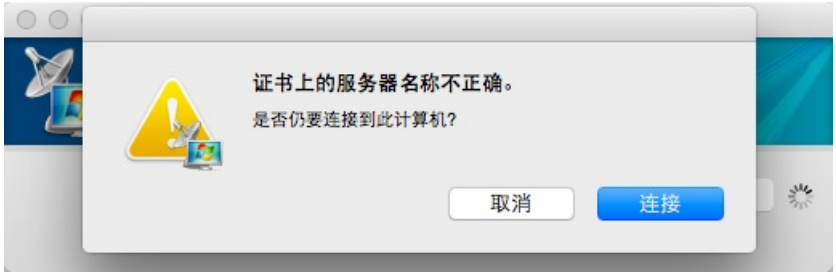
   > **说明** 其中，*<云盾堡垒机系统的IP>*指代云盾堡垒机系统的IP地址，请根据实际情况输入。

   通过远程桌面连接登录云盾堡垒机系统

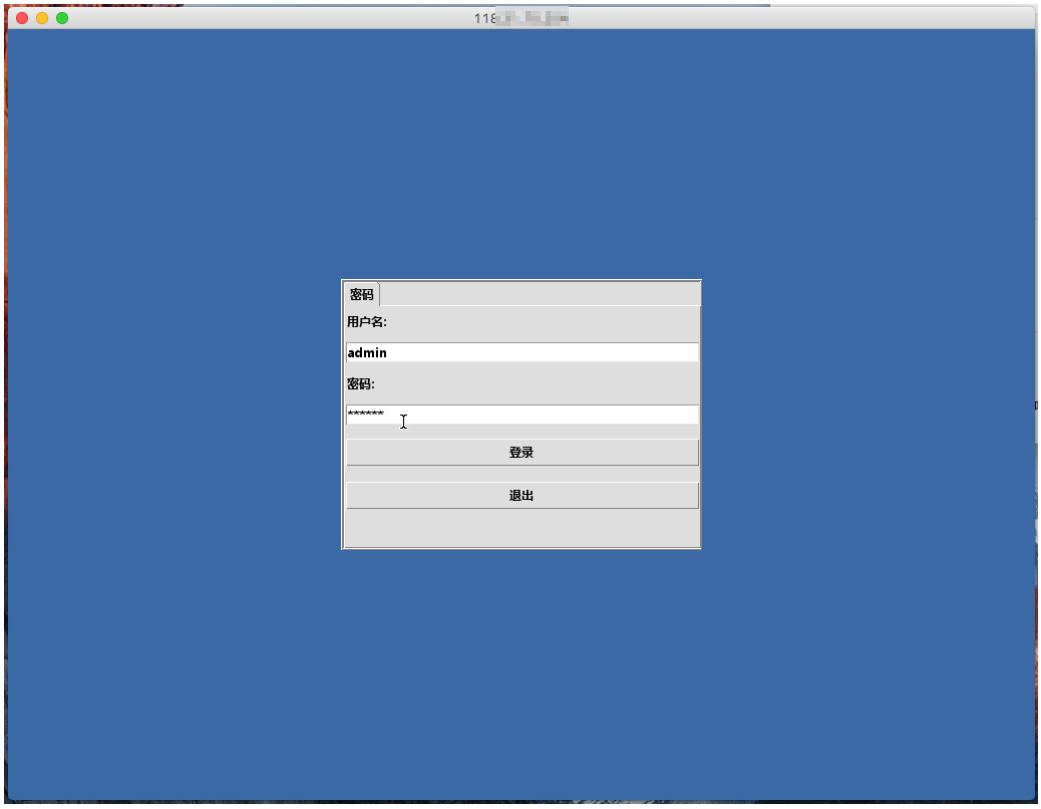
2. 在**是否仍要连接此计算机？**对话框中，单击**连接**。

   通过远程桌面连接连接云盾堡垒机系统

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**。

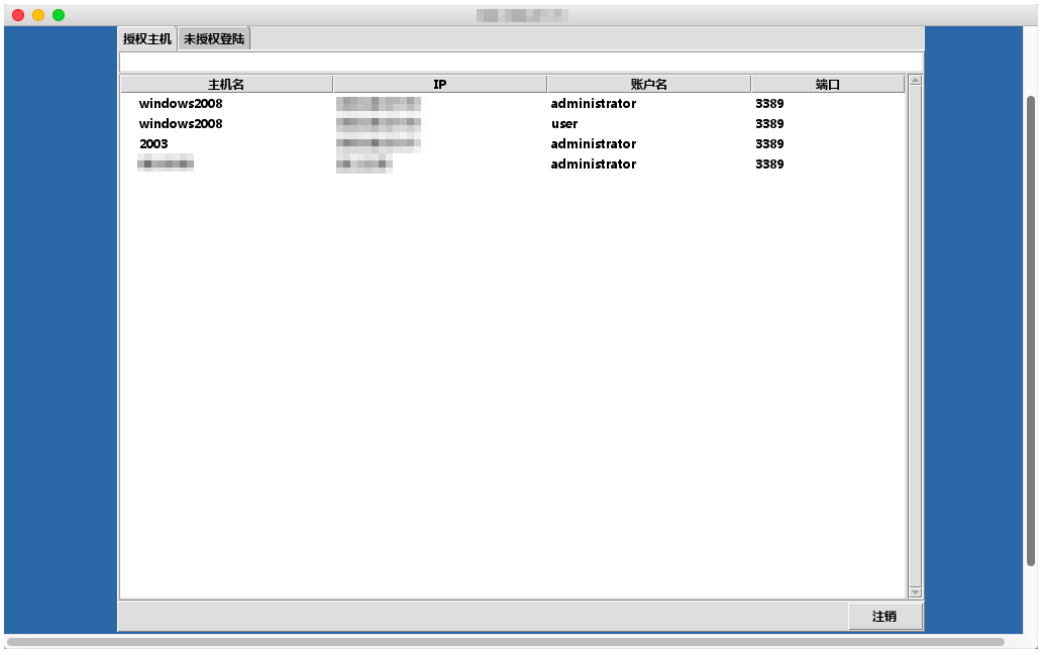
   登录云盾堡垒机系统



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。

> **说明** 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。

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。

10.8.4.3.2. 在Windows操作系统上运维

10.8.4.3.2.1. 准备工作

该章节介绍在Windows系统上使用云盾堡垒机运维需要的一些准备工作。

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。

10.8.4.3.2.2. 通过SSH工具登录目标主机进行运维

本章节以PuTTY工具为例，通过SSH协议登录目标主机进行运维。

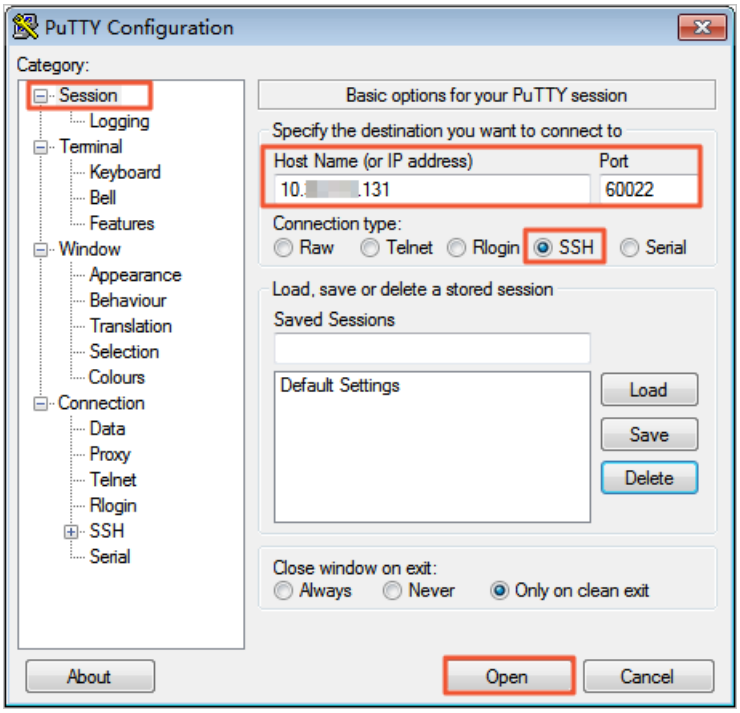
背景信息

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

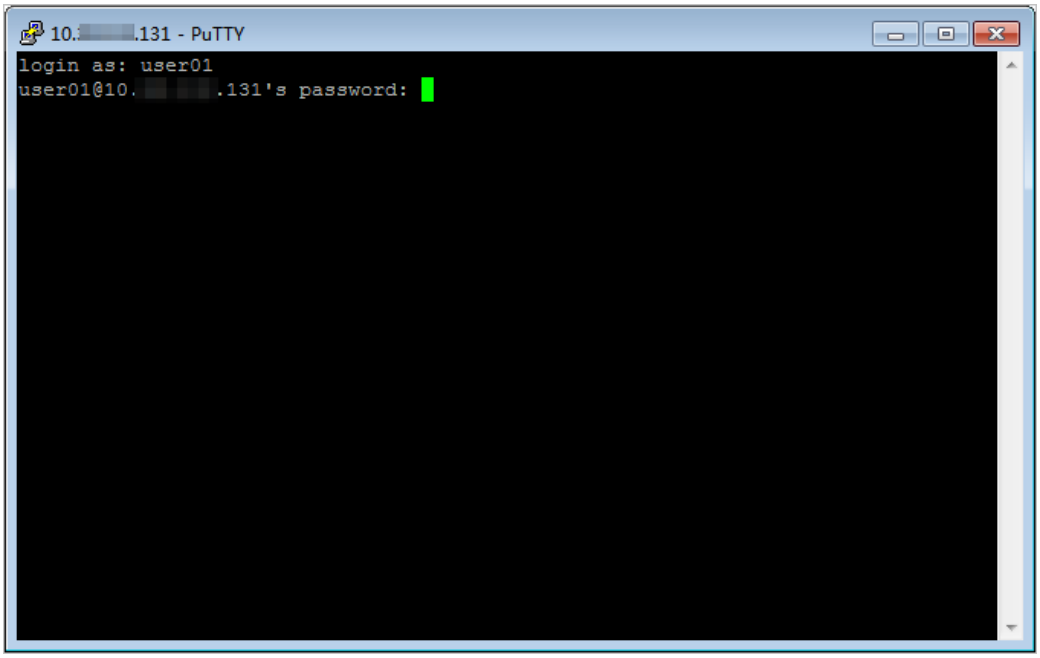
1. 打开PuTTY工具，在登录窗口中输入云盾堡垒机系统的IP和端口号（60022），单击**Open**。

   连接云盾堡垒机



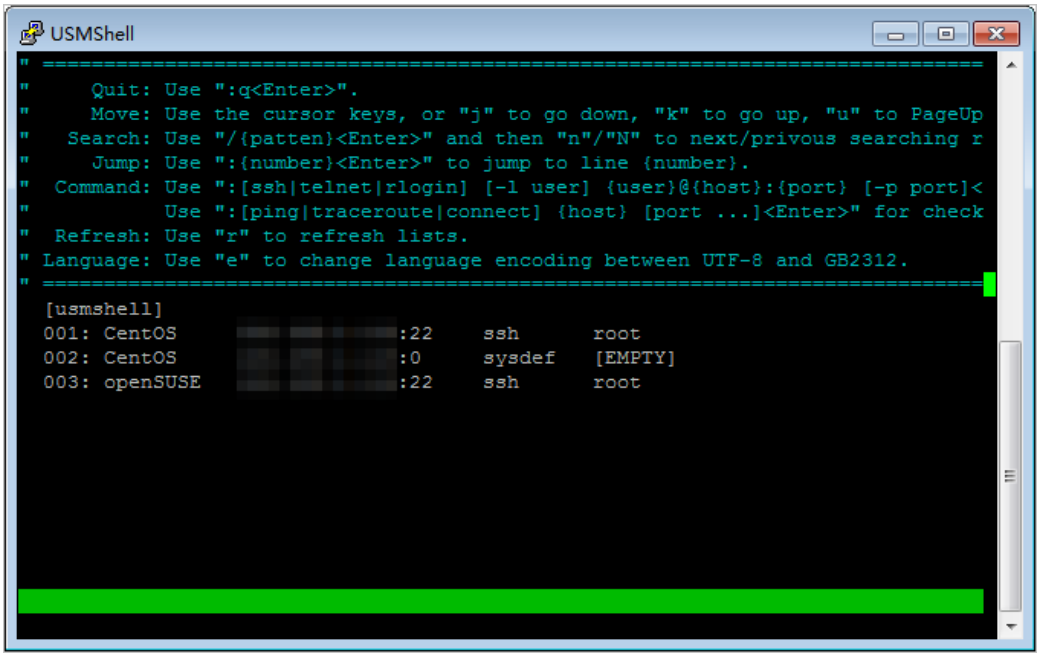
2. 输入云盾堡垒机系统的用户名和密码，按回车键（Enter）。

   登录云盾堡垒机



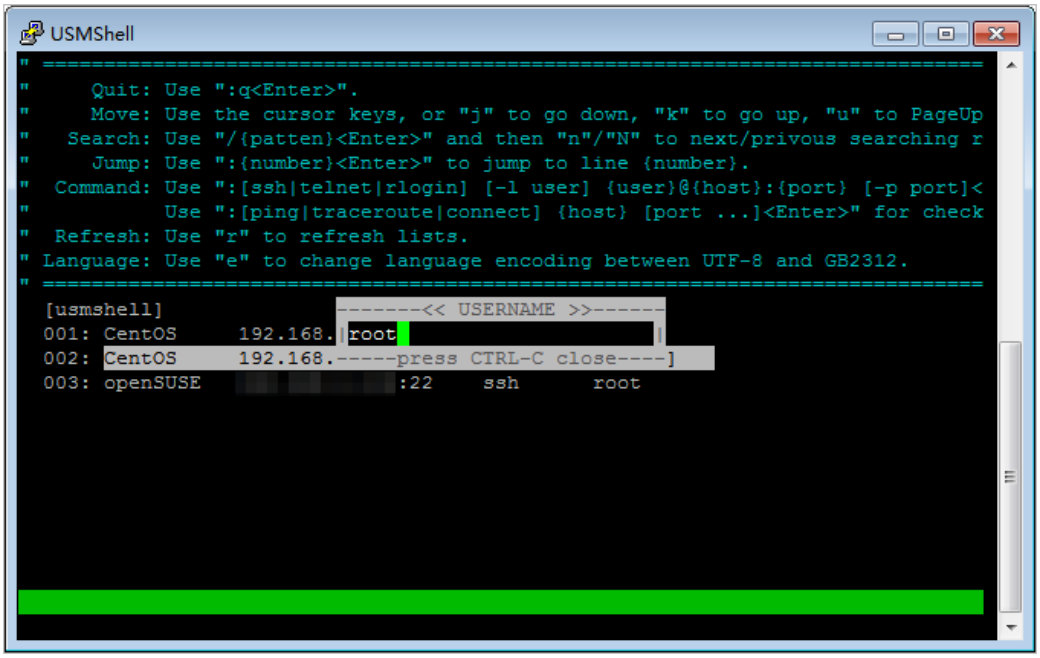
3. 进入资产管理界面，通过上下键选择已授权的主机资产。

   选择主机资产



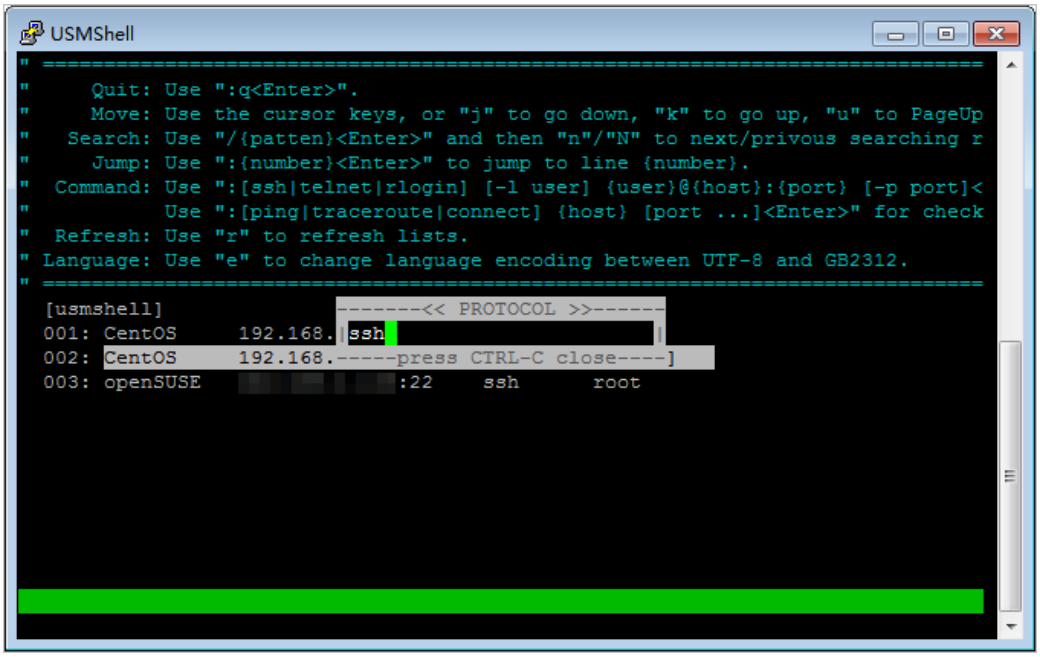
4. 在USERNAME中输入*主机帐户*，按回车键（Enter）。

   输入主机帐户



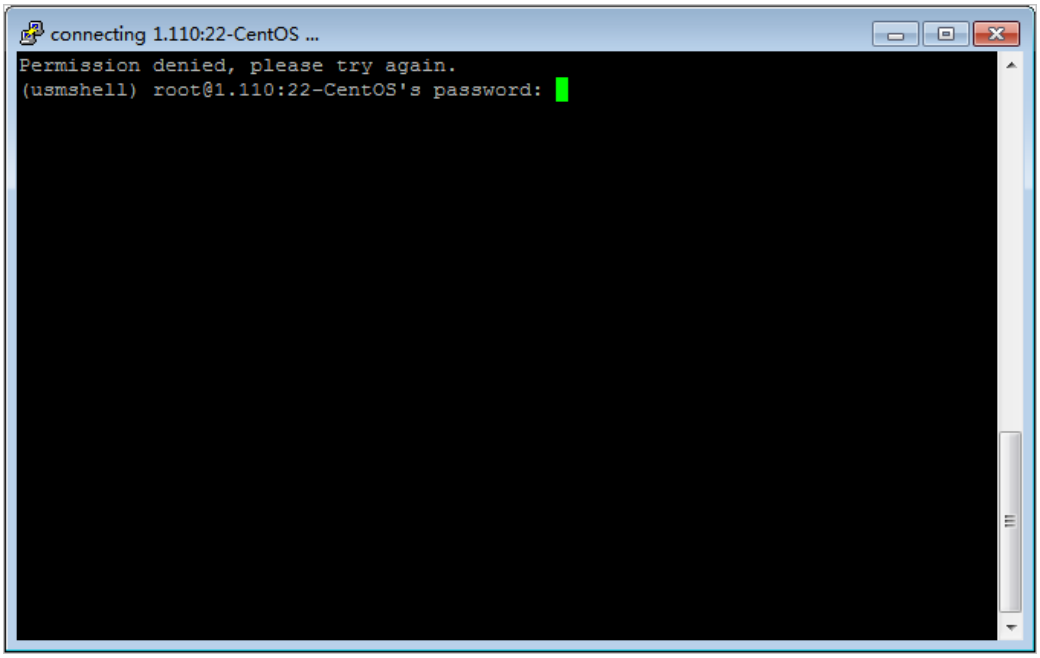
5. 在PROTOCOL中，输入*ssh*，按回车键（Enter）。

   输入SSH协议



6. 在主机登录界面，输入主机帐户的密码，按回车键（Enter）。

   输入主机帐户密码



登录目标主机进行运维操作。

10.8.4.3.2.3. 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

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。

背景信息

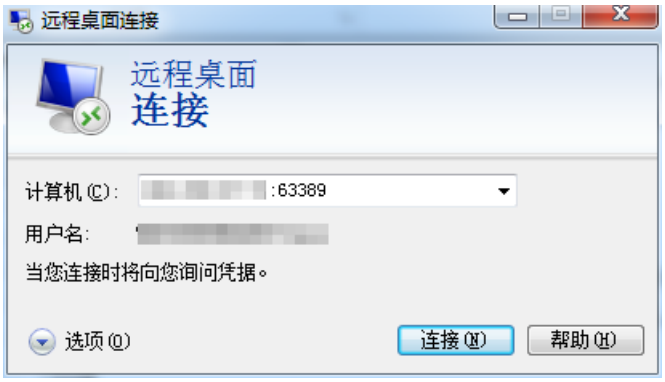
您可以参考本章节中的操作步骤使用其它运维工具登录RDP协议的主机帐户。

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**。

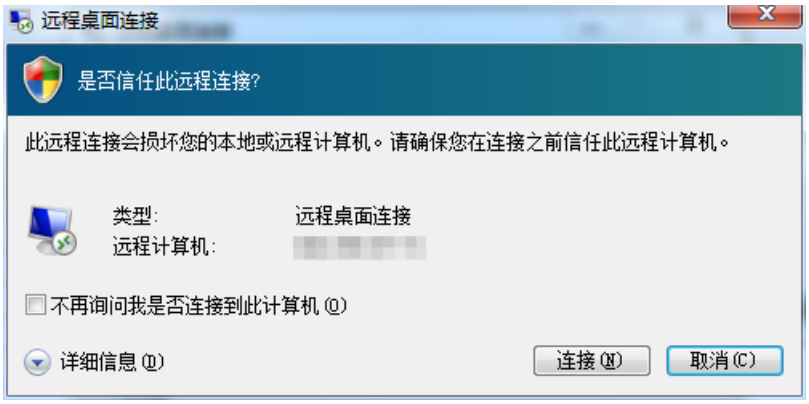
   > **说明** 其中，*<云盾堡垒机系统IP>*指代云盾堡垒机系统的IP地址，请根据实际情况输入。

   通过远程桌面连接工具登录云盾堡垒机系统

2. 在**是否信任此远程连接？**对话框中，单击**连接**。

   通过远程桌面连接工具连接云盾堡垒机系统

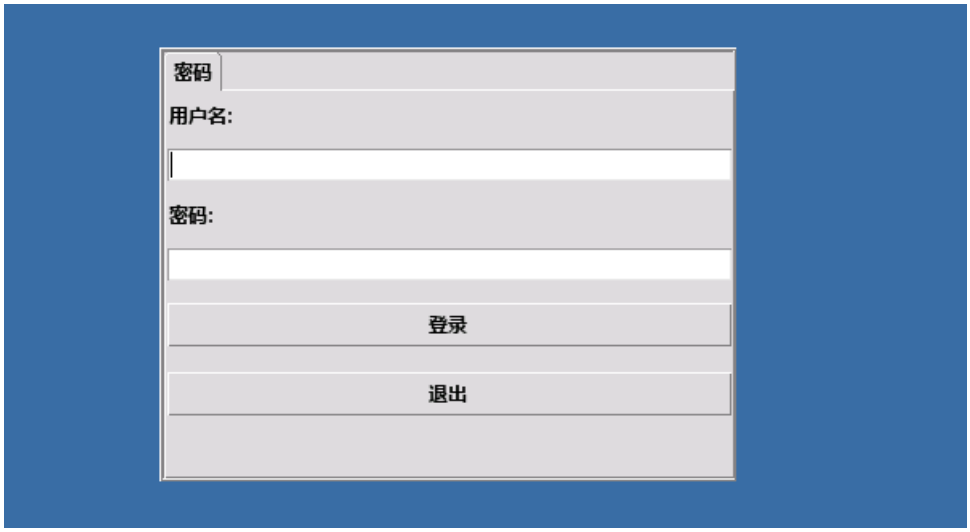
3. 在**无法验证次远程计算机的身份。是否仍要连接？**对话框中，单击**是**。

   通过远程桌面连接工具连接云盾堡垒机系统



4. 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**。

   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。

   > **说明** 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。

   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。

10.8.4.3.2.4. 通过WinSCP工具登录目标主机进行运维

本章节以WinSCP工具为例，通过SFTP协议登录目标主机进行运维。

背景信息

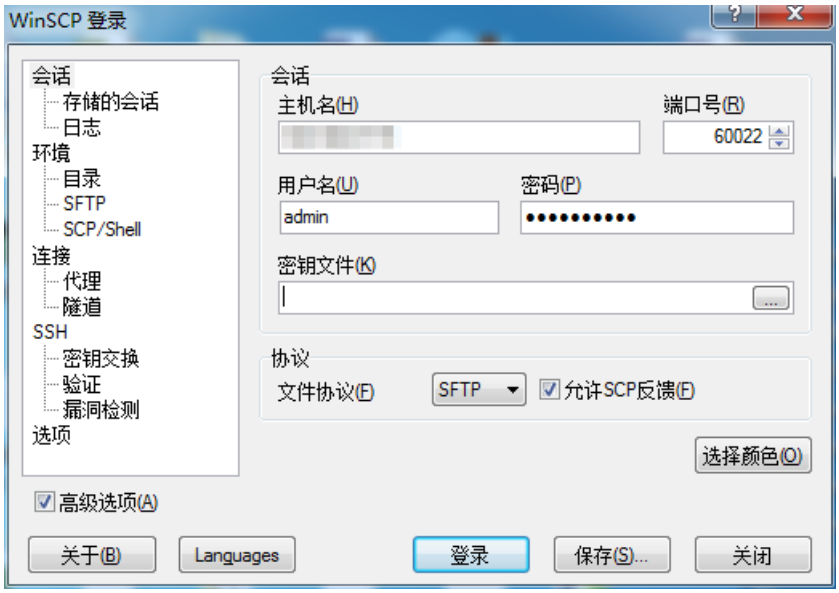
您可以参考本章节中的操作步骤使用其它运维工具登录SFTP协议的主机帐户。

> **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

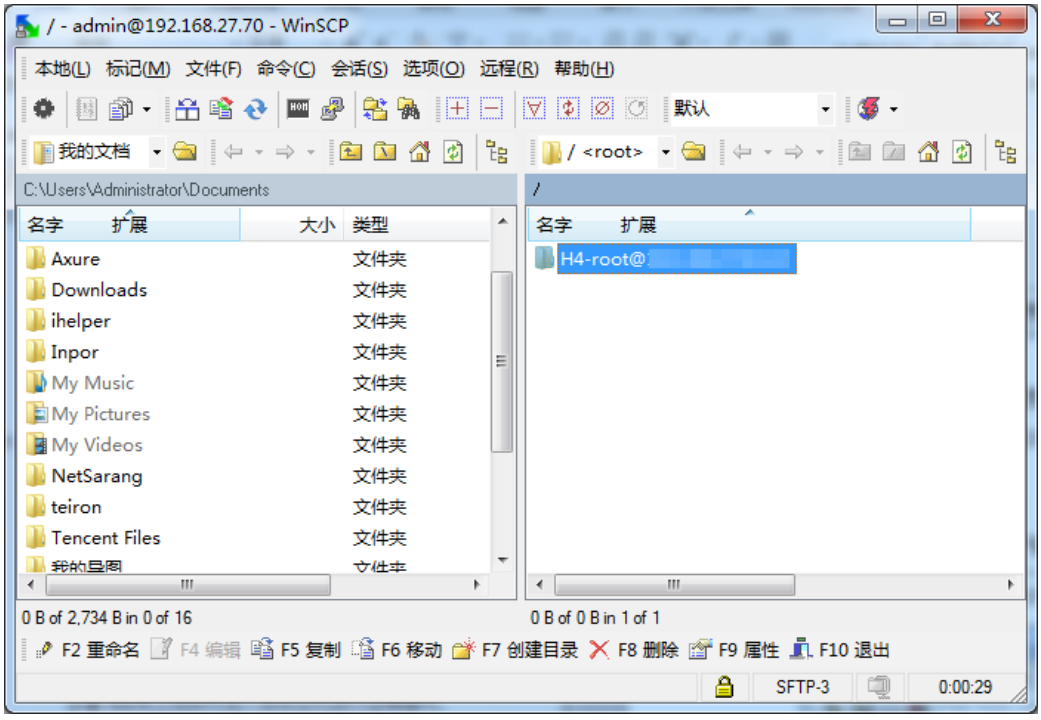
1. 打开WinSCP工具，在登录窗口中输入云盾堡垒机系统的IP、端口号（60022）、用户名、密码，单击**登录**。

   通过WinSCP工具登录云盾堡垒机系统



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。

   通过WinSCP工具选择主机资产



登录目标主机进行文件传输操作。

10.8.4.3.2.5. 通过XFTP工具登录目标主机进行运维

本章节以XFTP工具为例，通过FTP协议登录目标主机进行运维。

背景信息

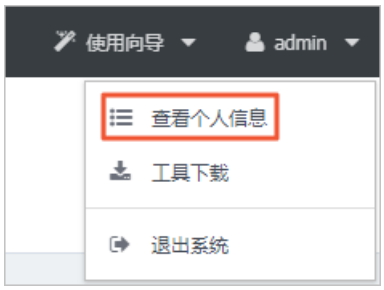
您可以参考本章节中的操作步骤使用其它运维工具登录FTP协议的主机帐户。

> **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. 使用运维员账号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**。

   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**。

   > **说明** CS登录口令用于以FTP客户端登录系统。

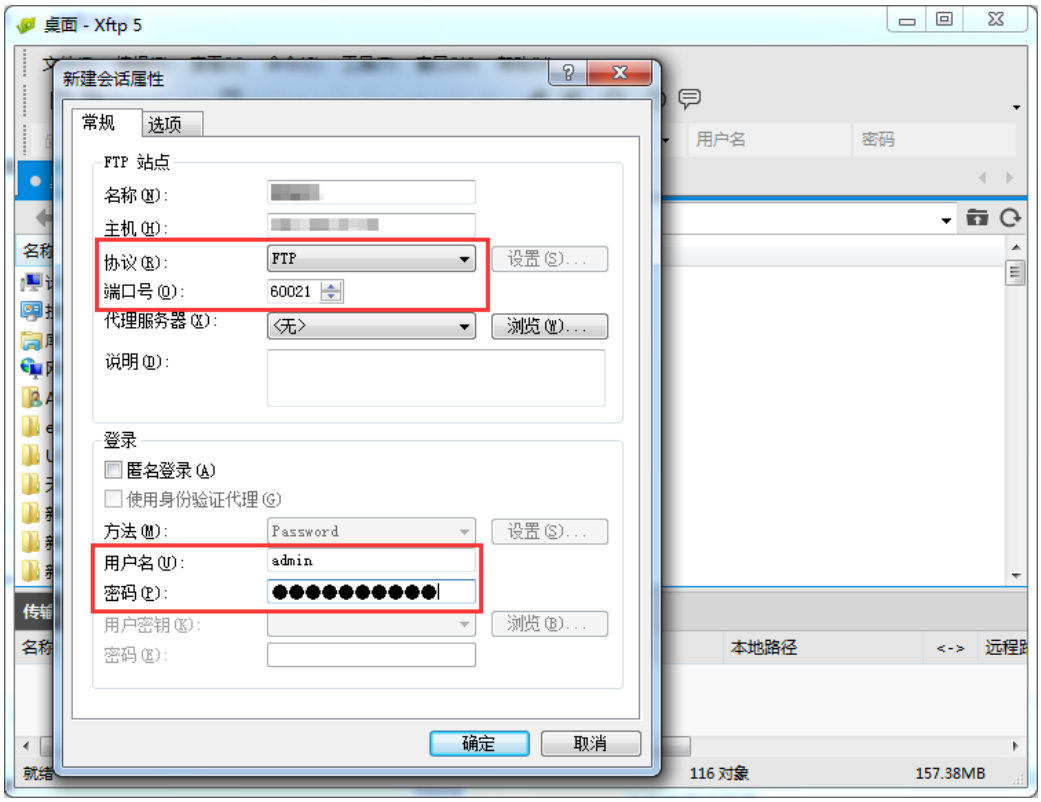
设置CS登录口令



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**。

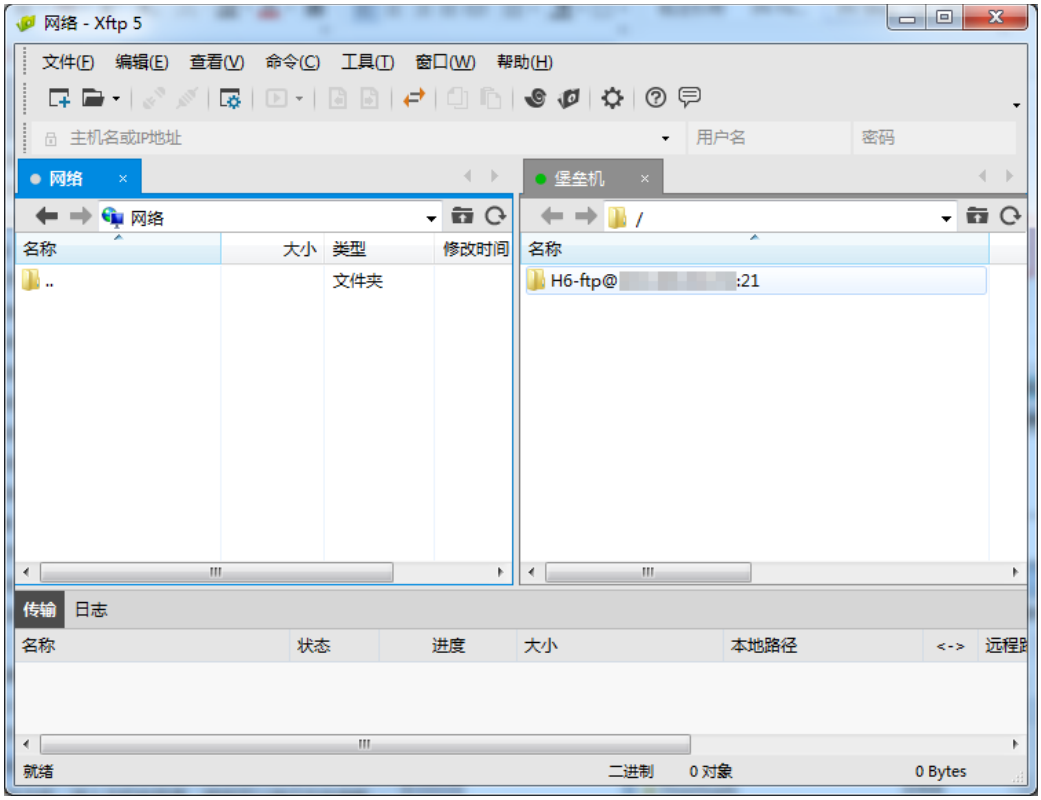
> **说明** 此处的密码需填写在上述步骤中设置的CS登录口令。

通过XFTP工具登录云盾堡垒机



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。

通过XFTP工具选择主机资产



登录目标主机进行文件传输操作。

10.8.4.4. 新建工单

该章节介绍运维人员如何新建工单。

背景信息

当运维人员需要运维授权关系以外的主机，且管理员并没有开启未授权登录时，运维人员可以通过工单向管理员申请运维这些资产。管理员批准工单后系统将自动创建工单中的授权关系。

操作步骤

1. 使用运维员账号登录云盾堡垒机系统。
2. 定位到**工单 > 我的工单**页面。
3. 单击**新建工单**。
4. 填写**授权有效期**和**备注**等信息。
5. 添加运维的资产。
   i. 单击**选择资产**。
   ii. 在列表中勾选主机帐户或应用。
   iii. 单击**添加**。
6. 单击**创建工单**。

   创建完成后，可以在**我的工单**页面查看自己所申请的工单信息，此时工单处于待审批的状态。
7. 管理工单信息。

   在待审批状态的工单，运维人员可以进行修改工单信息或者取消工单申请。

- 修改工单信息

  单击工单号或工单后的**详情**即可对工单进行修改。

- 取消工单申请

  勾选相应的工单条目，单击**取消**即可取消工单申请。

> 说明 已审批的工单不能取消或修改。

后续步骤

运维人员申请工单后，需要管理员审批工单，具体请参考审批运维工单。

审批通过后，运维人员可以在**运维**页面登录申请的主机。

10.8.5. 审计管理员操作指南

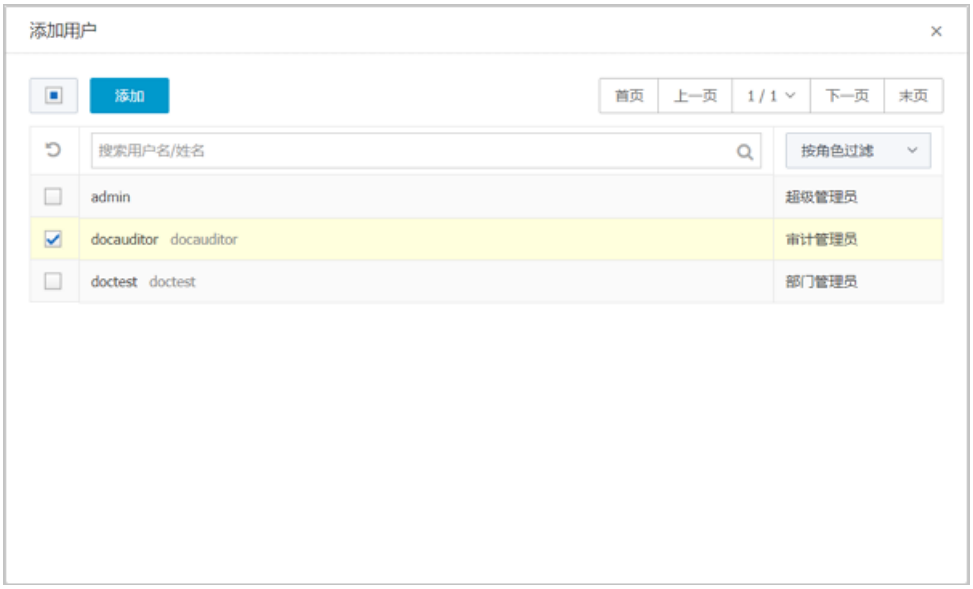
10.8.5.1. 审计规则

10.8.5.1.1. 添加审计规则

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。

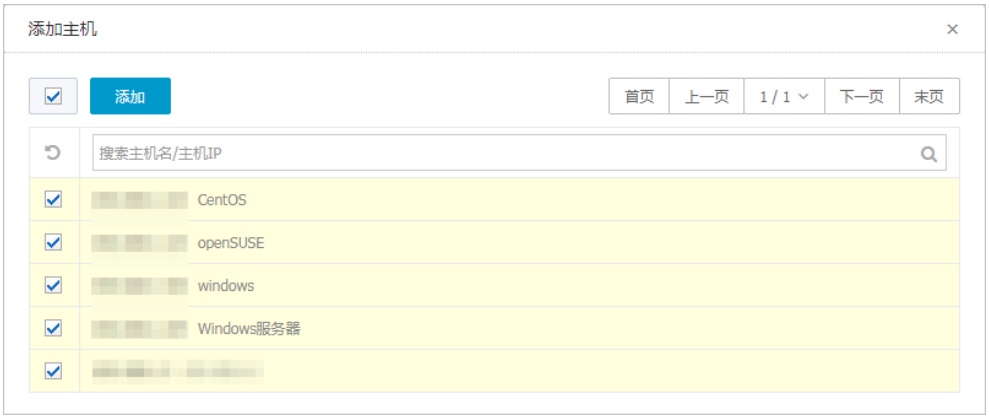
操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**审计** > **审计规则** 页面。
3. 选择**事件查询**页签，单击**新建审计规则**。
4. 在**新建审计规则**页面，在**名称**中填写审计规则名称。
5. 在**新建审计规则**页面，添加对应的审计用户。
   i. 单击**添加用户**。
   ii. 在**添加用户**对话框中勾选审计人员。



iii. 单击**添加**。

6. 在**新建审计规则**页面，添加被审计的主机。
   i. 单击**添加主机**。
   ii. 在**添加主机**对话框中勾选被审计的主机。



   iii. 单击**添加**。
7. 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。

后续步骤

审计规则创建完成后，在**审计规则**页面，可对审计规则进行修改和删除。

- 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。

10.8.5.2. 会话审计

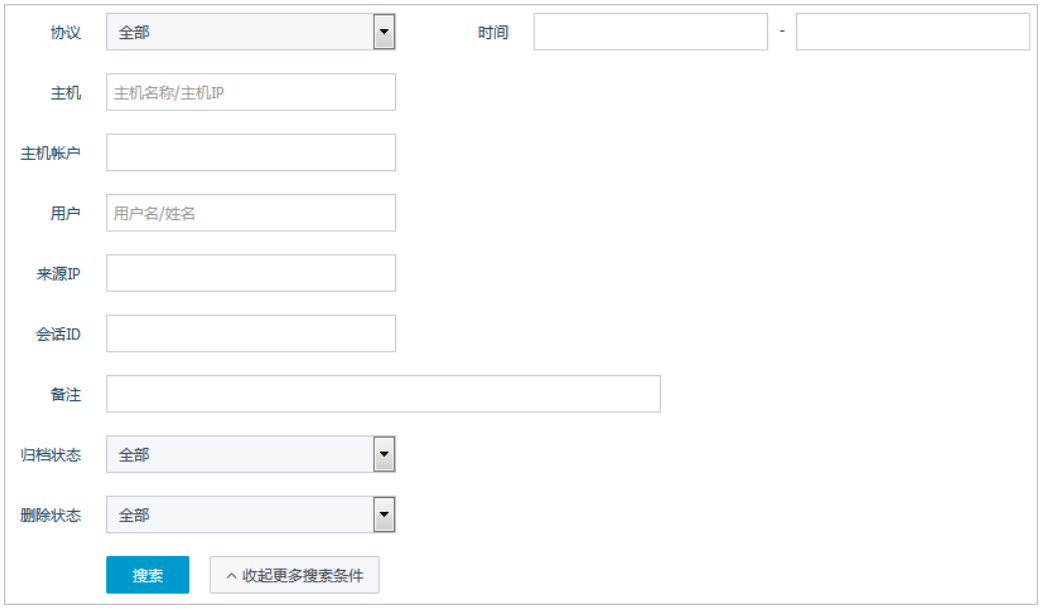
10.8.5.2.1. 搜索审计会话

该章节介绍通过搜索功能，快速查找符合条件的审计会话。

操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**审计 > 会话审计** 页面。
3. 选择**所有会话**页签，单击**展开更多搜索条件**。

   会话审计搜索条件



4. 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。

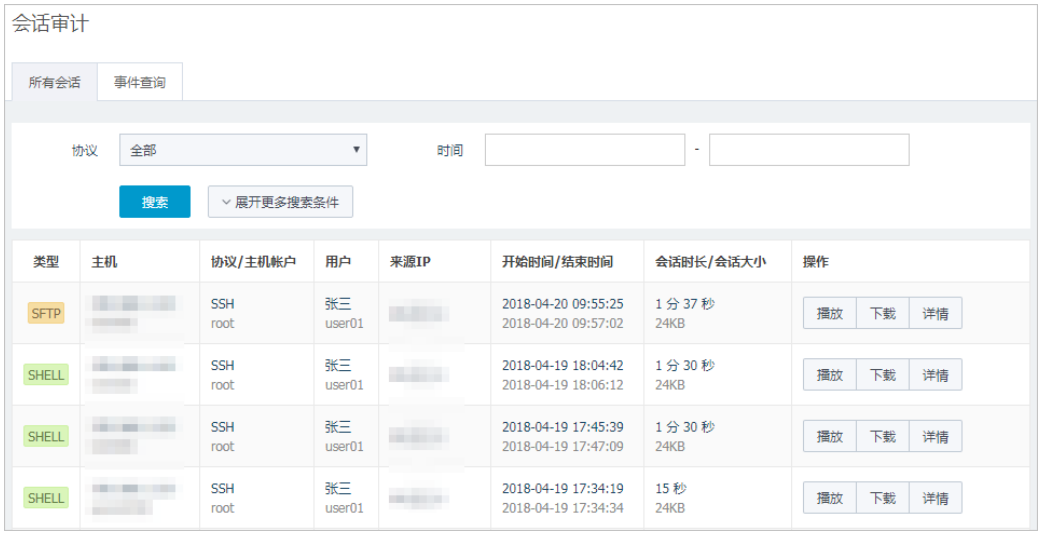
10.8.5.2.2. 查看所有会话

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

操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**审计 > 会话审计** 页面。
3. 选择**所有会话**页签，查看字符、图形、文件、应用类型的会话审计日志。

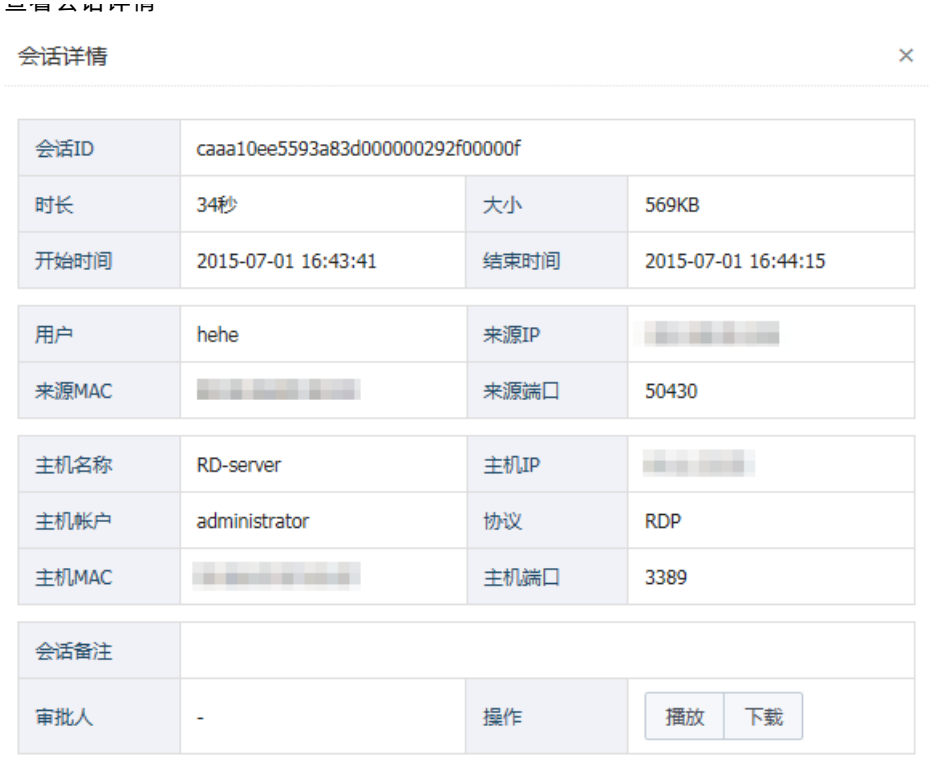
   查看所有会话



4. 选择会话日志，执行更多审计操作。
   - 查看详情：

     单击操作栏中的**详情**，可查看详细的会话信息。

     查看会话详情



- 下载会话文件：

  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。

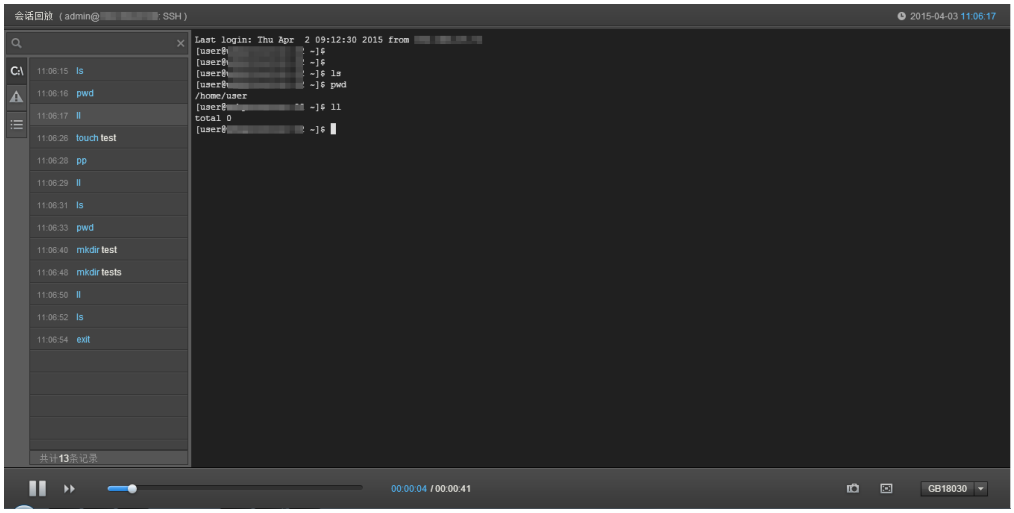
  > **说明** 在本地播放会话文件需安装离线播放器和Adobe AIR 4.0工具，参考下载运维工具下载并安装相关软件。

- 播放会话回放：

  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。

  > **说明** 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，参考下载运维工具下载并安装相关软件。

  查看会话审计回放



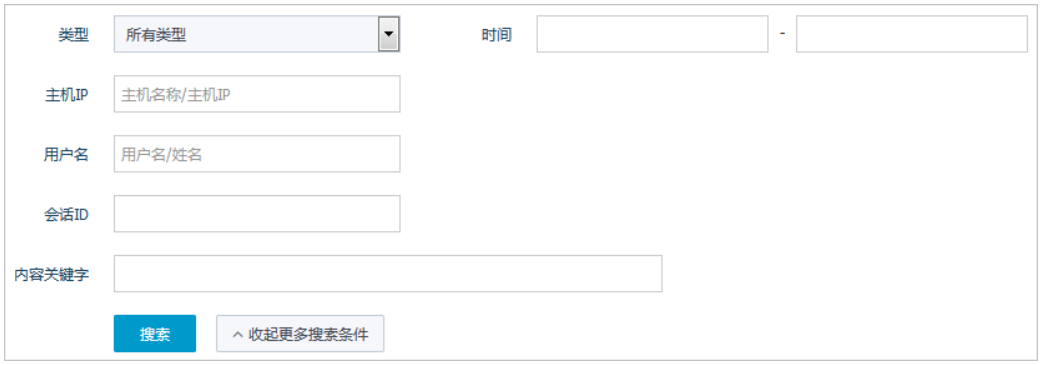
10.8.5.2.3. 搜索事件

该章节介绍通过搜索功能，快速查找符合条件的事件。

操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**审计 > 会话审计** 页面。
3. 选择**事件查询**，单击**展开更多搜索条件**。

   事件查询搜索条件



4. 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。

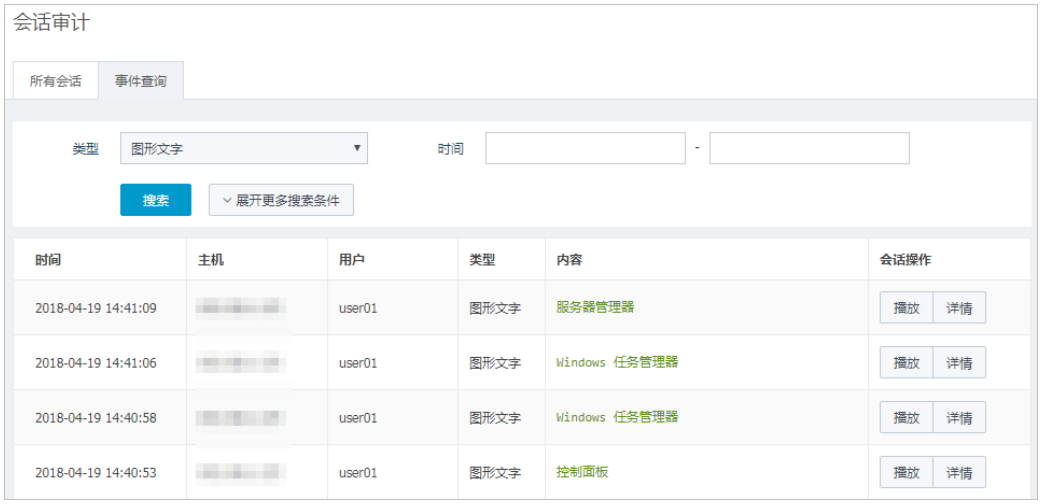
10.8.5.2.4. 查询事件

该章节介绍如何查看运维会话事件。

操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**审计 > 会话审计** 页面。
3. 选择**事件查询**，查看会话事件。

   查看运维事件



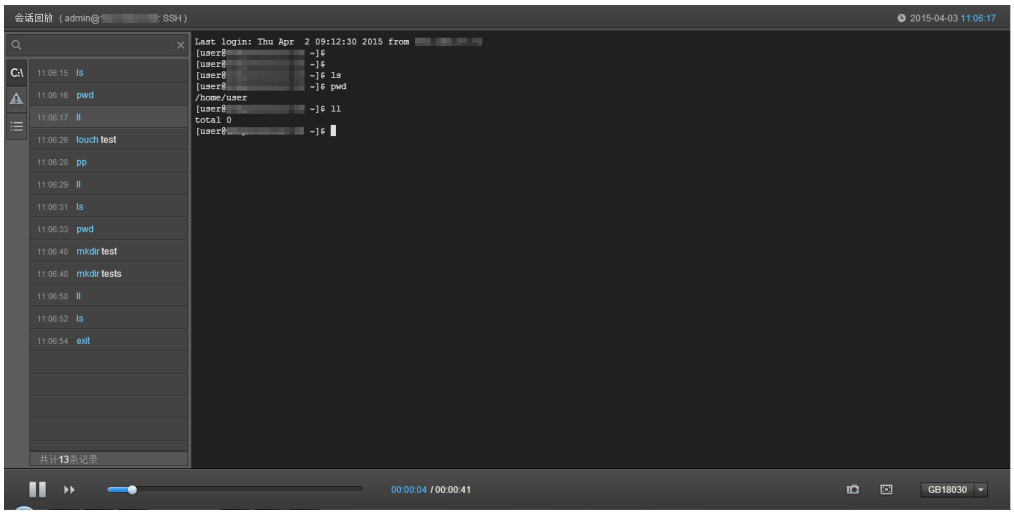
4. 选择会话事件，执行更多操作。
   - 查看事件详情：

     单击会话操作栏中的**详情**，可查看详细的会话信息。
   - 播放事件回放：

     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。

     > **说明** 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，参考下载运维工具下载并安装相关软件。

     查看会话审计回放



10.8.5.3. 运维报表

10.8.5.3.1. 按时间范围查看运维报表

运维报表用于统计当前用户的运维信息。

操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**运维 > 运维报表** 页面。



3. 选择需要查看的运维用户。
   i. 单击**用户**。
   ii. 在**选择用户**对话框，勾选需要查看的运维用户。
   iii. 单击**确定**。
4. 设置查看的时间范围。

   支持以下两种方式设置时间范围。
   - 在**日期**中，选择起始时间和结束时间。
   - 单击**今日**、**昨天**、**本周**和**本月**，自动选择时间段。

   选择后，页面自动刷新。
5. 选择页签，可查看不同类型的运维统计信息。
6. 在**导出报表**下拉菜单中，选择报表格式，导出该运维报表。

10.8.5.3.2. 设置报表自动发送

该章节介绍如何把运维报表周期性的发送给审计管理员和部门管理员。

前提条件

相应的审计管理员和部门管理员已在**用户信息**页面中设置邮箱信息。

操作步骤

1. 使用审计管理员账号登录云盾堡垒机系统。
2. 定位到**运维 > 运维报表** 页面。
3. 单击页面右上角的**报表自动发送**。
4. 在**报表自动发送**对话框中，配置相关设置项。

   设置报表自动发送



配置项	说明
状态	可选择*开启*、*关闭*。 如果需要使用报表自动发送功能，则选择*开启*。
发送周期	报表自动发送的周期。
文档格式	报表的格式，支持*ODC*、*PDF*和*HTML*。

5. 单击**确定**。

执行结果

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。

10.8.6. 系统管理员操作指南

10.8.6.1. 网络设置

10.8.6.1.1. 配置网络信息

该章节介绍如何配置云盾堡垒机系统的网络。

背景信息

通过配置堡垒机的网络设置，确保堡垒机网络连通性。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统** > **网络设置** > **网络设置**页面。

3. 查看堡垒机的网络接口信息。

   网络接口信息包括**接口名称**、**速度**、**连通状态**、**IP地址**、**子网掩码**等信息。

4. 设置DNS解析服务器。

   DNS服务器用于域名地址的解析。

   i. 在**DNS信息**中，配置DNS服务器。

   ii. 单击**保存更改**。

5. 配置协议端口。

   设置维护的各协议端口，并选择是否启用协议。

   i. 在**协议端口**中，支持修改系统的默认运维端口。

   ii. 设置需要支持的某协议，勾选启用框。

   iii. 单击**保存更改**。

6. 配置SSH协议。

   i. 在**SSH端口配置**中，勾选启用，同时支持修改系统默认管理端口。

   ii. 单击**保存更改**。

10.8.6.1.2. 配置Web

该章节介绍如何设置堡垒机的Web服务。

背景信息

通过Web设置，启用HTTPS服务，保障堡垒机的安全性。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 网络设置 > Web设置**页面。
3. 修改Web端口。

   i. 在**Web设置**区域，设置Web端口、配置是否启用**增强HTTPS安全性**。

   ii. 单击**保存更改**。

4. 配置Web证书。

   i. 在**Web证书配置**区域，输入**系统IP**。

   ii. 单击**保存更改**。

5. 自定义Web证书。



i. 在**自定义Web证书**区域，上传证书及私钥等信息。

ii. 单击**保存更改**。

10.8.6.1.3. 配置静态路由

该章节介绍如何配置静态路由。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 网络设置 > 静态路由配置**页面。
3. 在**新建路由规则**中填写路由相关信息。
4. 单击**创建路由规则**。

10.8.6.1.4. 配置SNMP

该章节介绍如何配置SNMP。

背景信息

SNMP（Simple Network Management Protocol，简单网络管理协议）是广泛应用于TCP/IP网络的网络管理标准协议。SNMP提供了一种通过运行网络管理软件的网络管理设置来管理堡垒机的方法。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 网络设置 > SNMP**页面。

3. 在**SNMP配置**中设置SNMP状态及信息，单击**保存更改**。
4. 在**新建只读社团**中，设置社团名称、SNMP版本、IP限制，单击**创建社团**。
5. 在**常用节点信息**中，查看SNMP输出的OID信息。

10.8.6.1.5. 配置IP源防护

该章节介绍如何配置IP源防护，限制登录到堡垒机的IP。

背景信息

IP源防护主要用于对来源地址限制访问堡垒机。当不需要防护时，将防护模式设置为关闭；需要防护时分为两种防护模式：

- 黑名单模式开启时，列入黑名单的IP地址将不允许访问堡垒机。
- 白名单模式开启时，只有列入白名单的IP地址可以进行访问堡垒机。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 网络设置 > IP源防护**页面。
3. 在**基本设置**中，设置**防护模式**，单击**保存更改**。
   - **防护模式**设置为*黑名单模式*，后续参考步骤。
   - **防护模式**设置为*白名单模式*，后续参考步骤。
4. 设置黑名单模式。
   i. 在**黑名单IP列表**中，单击**添加黑名单IP**。
   ii. 设置黑名单IP及备注信息。
   iii. 单击**添加到IP列表**。
   如果需要移除黑名单，则直接在列表后面单击**删除**。
5. 设置白名单模式。
   i. 在**白名单IP列表**中，单击**添加白名单IP**。
   ii. 设置白名单IP及备注信息。
   iii. 单击**添加到IP列表**。
   如果需要移除白名单，则直接在列表后面单击**删除**。

10.8.6.2. 认证管理

10.8.6.2.1. 配置安全设置

通过该章节介绍如何配置用户登录时的安全策略。

背景信息

通过配置堡垒机登录限制、锁定策略和密码策略，保障堡垒机的安全。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。

2. 定位到**系统 > 认证管理 > 安全配置**页面。
3. 设置登录限制条件。
   i. 在**登录配置**页面，编辑登录超时时间、验证码过期时间以及admin账户限制。
      - **登录超时**：当用户超过设定时长没有操作时，再次操作需要重新登录。
      - **验证码**：在登录时，是否启用验证码验证，及验证码过期时间。
      - **限制**：是否禁止admin从Web登录。
   ii. 单击**保存更改**，即可生效。
4. 设置用户锁定策略。
   i. 在**用户锁定**页面，编辑用户锁定策略。
      - **密码尝试次数**：当用户密码输入错误次数超过设定值时，锁定该用户。
      - **锁定时长**：用户被锁定后，超过该设置时长后才能正常操作。
      - **重置计数器**：输入错误密码后，将登录尝试失败计数器重置为0次所需要的时间。
   ii. 单击**保存更改**，即可生效。
5. 设置用户密码策略。
   i. 在**用户密码配置**页面，编辑用户密码策略。
      - **密码策略**：是否强制使用强密码。
      - **密码使用期限**：密码超过设定期限后，需要修改密码才能正常使用。
   ii. 单击**保存更改**，即可生效。

10.8.6.2.2. 设置远程认证

该章节介绍如何设置远程认证。

背景信息

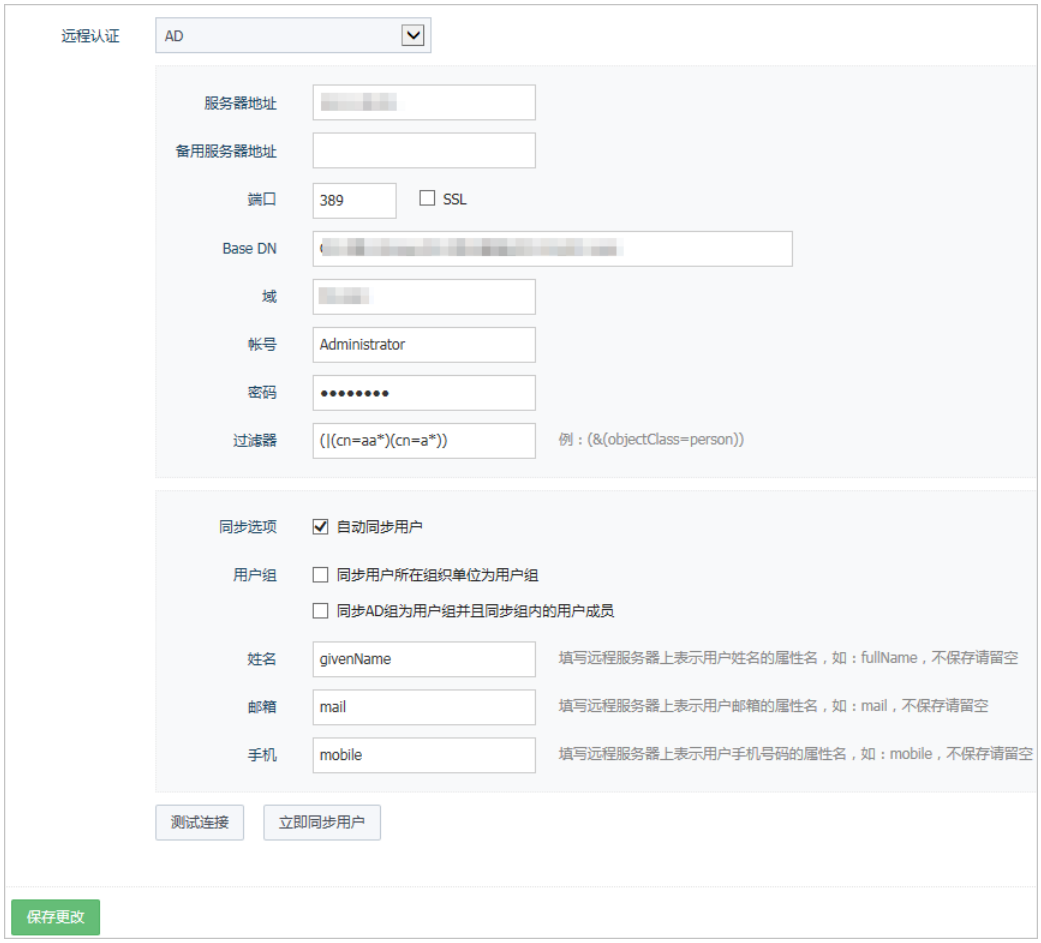
堡垒机支持AD、LDAP、RADIUS等远程认证方式。通过远程认证方式，统一对用户和密码进行管理，保障堡垒机的安全。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 认证管理 > 远程认证**页面。
3. 配置是否开启本地认证。

   在**本地认证**区域，选择是否开启本地认证功能。关闭后，用户将无法以本地认证方式登录。
4. 配置AD/LDAP远程认证。

   堡垒机与AD/LDAP服务器对接，可将AD/LDAP服务器用户同步到堡垒机，作为堡垒机用户使用。此功能需具有部署好的AD/LDAP环境，且保证堡垒机至服务器网络可达。



i. **远程认证**设置为*AD/LDAP*。

ii. 设置AD/LDAP服务器信息，单击**测试连接**，测试AD/LDAP服务器连通性。

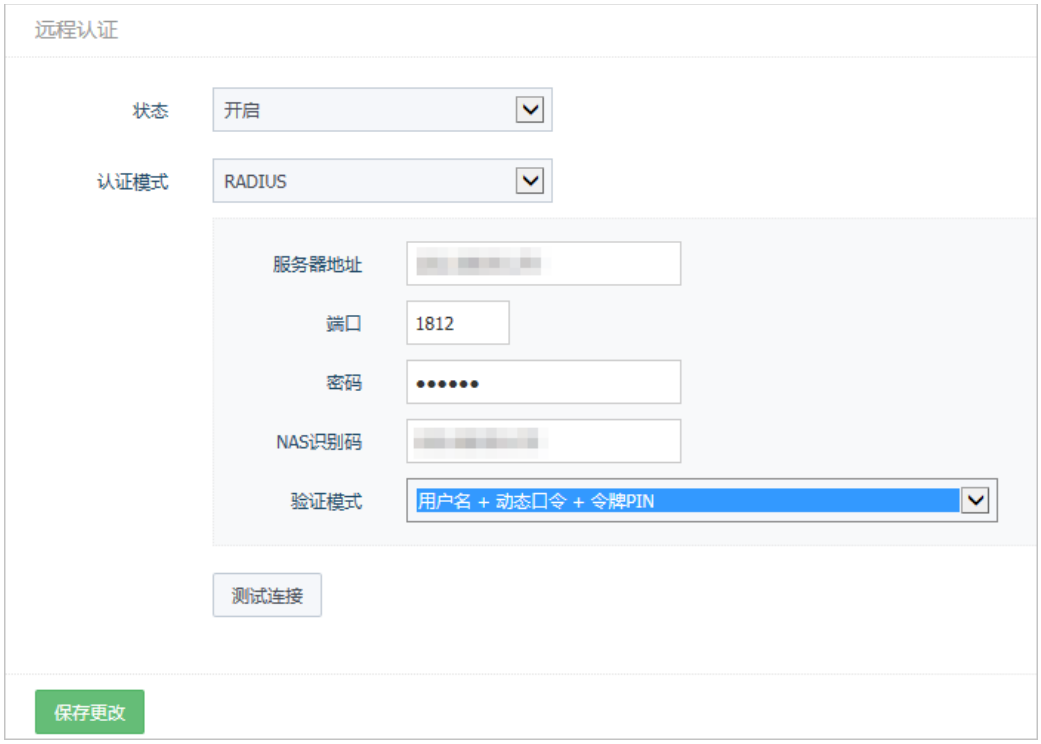
iii. 设置同步用户信息，单击**立即同步用户**，可将AD/LDAP服务器用户同步到堡垒机。

iv. 单击**保存更改**，完成AD/LDAP认证配置。

5. 配置RADIUS远程认证。

   RADIUS验证模式有三种：

   - 选择用户名和密码时，使用用户名和密码验证。
   - 选择用户名和动态口令时，可以使用用户名、密码或者动态口令验证。
   - 选择用户名、令牌PIN和动态口令时，可以使用用户名、密码验证，也可以使用用户名、令牌PIN和动态口令验证。



i. 在**远程认证**区域中，**状态**设置为*启用*，**认证模式**设置为*RADIUS*。
ii. 设置RADIUS服务器信息。
iii. 单击**测试连接**，测试RADIUS服务器连通性。
iv. 单击**保存更改**，完成RADIUS认证配置。

10.8.6.2.3. 配置双因子认证

该章节介绍如何配置双因子认证。

背景信息

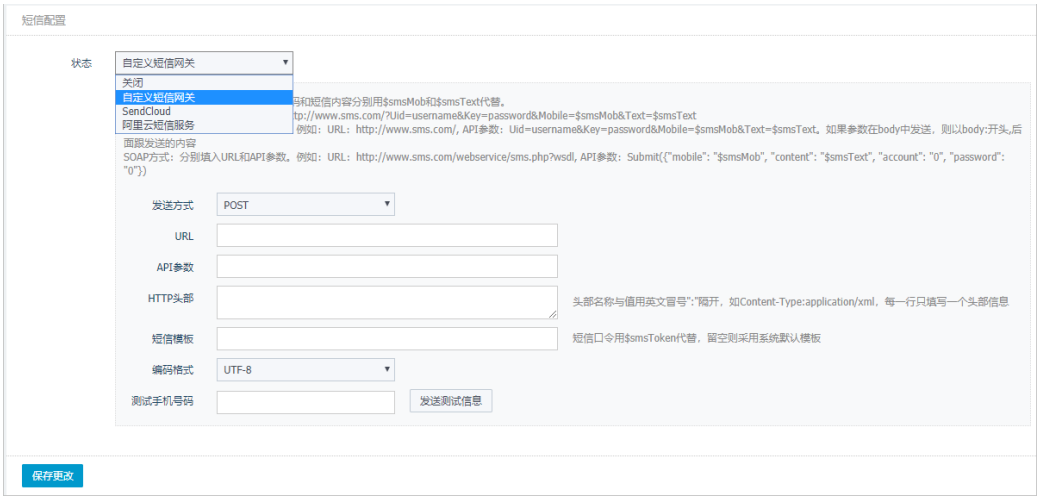
双因子认证机制，通过短信认证口令及手机APP口令技术，控制账号密码泄露风险，防止运维人员身份冒用和复用。开启双因子认证之后，运维人员登录堡垒机时，需要先输入用户密码，密码验证正确之后，再输入认证口令才能登录成功。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 认证管理 > 双因子认证**页面。
3. 选择双因子认证方式，单击**保存更改**。

   双因子认证方式支持*密码*、*手机APP令牌*、*短信口令*。
   - 当勾选了*密码*时，将优先采用密码认证方式，运维人员登录堡垒机时输入用户密码即可登录成功。
   - 仅勾选*短信口令*或*手机APP令牌*未勾选*密码*，运维人员登录堡垒机时，需要先输入用户密码，密码验证正确之后，再输入认证口令才能登录成功。
4. 设置短信网关，单击**保存更改**。

   如果双因子认证的**认证方式**选择了*短信口令*，则需要设置短信网关，用来发送认证短信。



i. 在**短信配置**区域，**状态**中选择需要使用的短信网关。

ii. 填写短信网关相关信息。

输入测试手机号码，单击**发送测试信息**，可以测试此短信网关是否可用。

iii. 单击**保存更改**。

10.8.6.3. 系统配置

10.8.6.3.1. 配置运维管理

该章节介绍如下配置运维管理，包括未授权登录，运维登录，SSH登录和运维时长限制配置等。

背景信息

通过运维配置，限制运维人员的登录方式、登录时长等，保障运维安全。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 系统配置 > 运维配置**页面。



3. 设置未授权登录配置。

   未授权运维配置主要是对未授权登录进行相关配置。当勾选了**允许未授权登录**，运维人员可以在**运维**页面，通过未授权登录运维自身授权关系以外的资产。

   - **收集未授权登录**：用户进行未授权登录后，系统会自动收集用户和主机的授权对应关系，在**未授权登录审核**页面可以查看。
   - **收集主机帐户的密码**：用户进行未授权登录后，系统会自动收集用户所登录主机的帐户和密码。
   - **自动创建运维规则**：系统检测到未授权登录的事件发生后，会自动创建相应授权关系，不需要管理员进行手动授权。

4. 设置运维登录配置。

   设置用户通过堡垒机登录运维目标主机时的方式：

   - **允许使用用户密码登录主机**：允许用户使用堡垒帐户登录主机。勾选此项后，在**运维**界面的帐户列表中会有相关项，如选用[SYSDEF][SELF]帐户，即可使用堡垒帐户登录主机。主要适用于用户和帐户同属于AD/LDAP的场景。
   - **允许使用用户SSH私钥登录主机**：勾选此项后，堡垒将允许用户无需输入主机帐户的密码，使用已经添加过的SSH私钥登录主机运维。
   - **允许使用SSH-agent-forwarding方式登录SSH服务器**：勾选此项后，堡垒将支持SSH-agent-forwarding 特性，适用于登录堡垒机和登录SSH服务器使用同样私钥的场景。

5. 设置SSH登录配置。

   设置用户登录堡垒机方式：

   - **允许使用公钥登录**：勾选此项后，用户可以使用SSH公钥登录堡垒机。
   - **允许使用密码登录**：勾选此项后，用户将通过密码登录堡垒机。

- **允许发送环境变量**：勾选此项后，用户可以选择允许发送运维用户信息和运维来源IP。
- **Usmshell使用命令行方式**：勾选此项后，将通过命令行方式登录堡垒机。

6. 设置运维时长限制。

   当协议连接上的空闲时长超过此限制，网络连接会自动断开，各协议空闲时长定义如下：

   - rdp、vnc：客户端无数据发送时。
   - ftp：命令通道和数据通道均无数据发送时。
   - ssh、telnet、sftp：客户端和服务端均无数据发送时。

10.8.6.3.2. 配置告警信息

该章节介绍如何配置堡垒机告警。

背景信息

堡垒机支持以邮件告警和Syslog告警的方式发送操作日志的告警信息，方便管理者接收相应的告警，并根据实际情况及时处理告警信息。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 系统配置 > 告警配置**页面。
3. 配置以邮件方式告警。
   i. 在**邮件配置**中，配置邮件信息。

      设置邮件发送方式、邮件服务器地址、端口、发件人帐号、收件人帐号等信息。

   ii. 单击**发送测试邮件**，测试邮件是否可达。

   iii. 单击**保存更改**，完成邮件方式告警。
4. 配置Syslog告警。
   i. 在**Syslog配置**中，配置Syslog信息。

      设置Syslog的发送者标识、服务器IP、端口等信息。

   ii. 单击**发送测试数据**，测试Syslog服务器是否连通。

   iii. 单击**保存更改**，完成Syslog方式告警。
5. 启用操作日志告警。
   i. 在**操作日志告警**中，**状态**选择*启用*。

   ii. 设置邮件告警和Syslog告警发送的告警等级。

      选择相关告警级别后，只发送对应级别的操作日志告警信息。

   iii. 单击**保存更改**。

10.8.6.3.3. 配置语言和界面

该章节介绍如何配置堡垒机的语言和界面。

背景信息

堡垒机支持简体中文、繁体中文和英文等语言。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 系统配置 > 语言和界面**页面。
3. 在**语言设置**中，选择语言类型。
4. 单击**保存更改**，修改界面语言。

10.8.6.3.4. 配置功能

该章节介绍是否启用报表自动统计功能。

背景信息

在**功能设置**页可设置是否开启报表自动统计，开报表自动统计后，可以提升报表页面数据加载效率，系统会在每日0点后自动统计前一周期的报表数据，会消耗一定系统CPU资源并持续一定时间，请按需设置。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 系统配置 > 功能设置**页面。
3. 在**报表自动统计**中，**状态**设置为*开启*。

   如果消耗资源影响堡垒机的性能，可设置为*关闭*，关闭该功能。
4. 单击**保存更改**。

10.8.6.3.5. 配置SSH KEY

该章节介绍如何配置SSH KEY。

前提条件

已经在客户端生成私钥。

背景信息

上传SSH KEY私钥，并且**系统 > 系统配置 > 运维配置**中已经启用**允许使用用户SSH私钥登录主机**，堡垒机可以通过SSH私钥方式登录运维目标。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 系统配置 > SSH KEY配置**页面。
3. 单击**上传新DSA私钥**。
4. 在**上传新DSA私钥**弹窗中，粘贴客户端生成的私钥内容。
5. 单击**上传DSA私钥**。

10.8.6.4. 存储管理

10.8.6.4.1. 数据归档

该章节介绍如何使用数据归档。

背景信息

通过数据归档管理操作，将录像进行归档，方便以后查看。同时支持删除数据功能，释放堡垒机的存储空间。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 存储管理 > 数据归档**页面。
3. 在**磁盘数据状态**区域，查看系统分区资源占用情况、会话分区资源占用情况和归档状态。
4. 设置开启或关闭录像归档功能。

   通过录像归档功能，将录像定时归档存储到远程服务器上，支持FTP和SFTP传输模式。



   开启归档功能操作如下：

   i. 在**录像归档**区域，设置*开启*状态。
   ii. 设置归档参数信息。
      - 设置归档时间段：设置每天归档的时段。
      - 设置归档传输参数：设置归档的速度限制和传输模式。
      - 设置归档存储的服务器信息：包括服务器地址、端口、用户名、密码和存储路径。
   iii. 单击**测试用户**，确认归档的存储服务器是否正常可用。
   iv. 单击**保存更改**。
5. 设置自动删除录像功能。
   i. 在**自动删除**区域，设置自动删除条件。

      系统可根据以下判断条件自动删除录像。
      - 设置保留天数，录像生成时间超过多少天时，自动删除录像。
      - 设置可用空间，在空间少于多少G时，自动删除录像。
      - 设置只删除已归档录像。
   ii. 单击**保存更改**。

6. 手动删除数据。
   i. 在**手工删除**区域，设置需要删除的数据。
      - 设置删除多少天前的数据。
      - 设置删除的内容，可选*操作日志*、*系统警报*、*录像*、*只删除已归档的录像*。
   ii. 单击**删除数据**，手动删除已选数据。

10.8.6.4.2. 录像导出

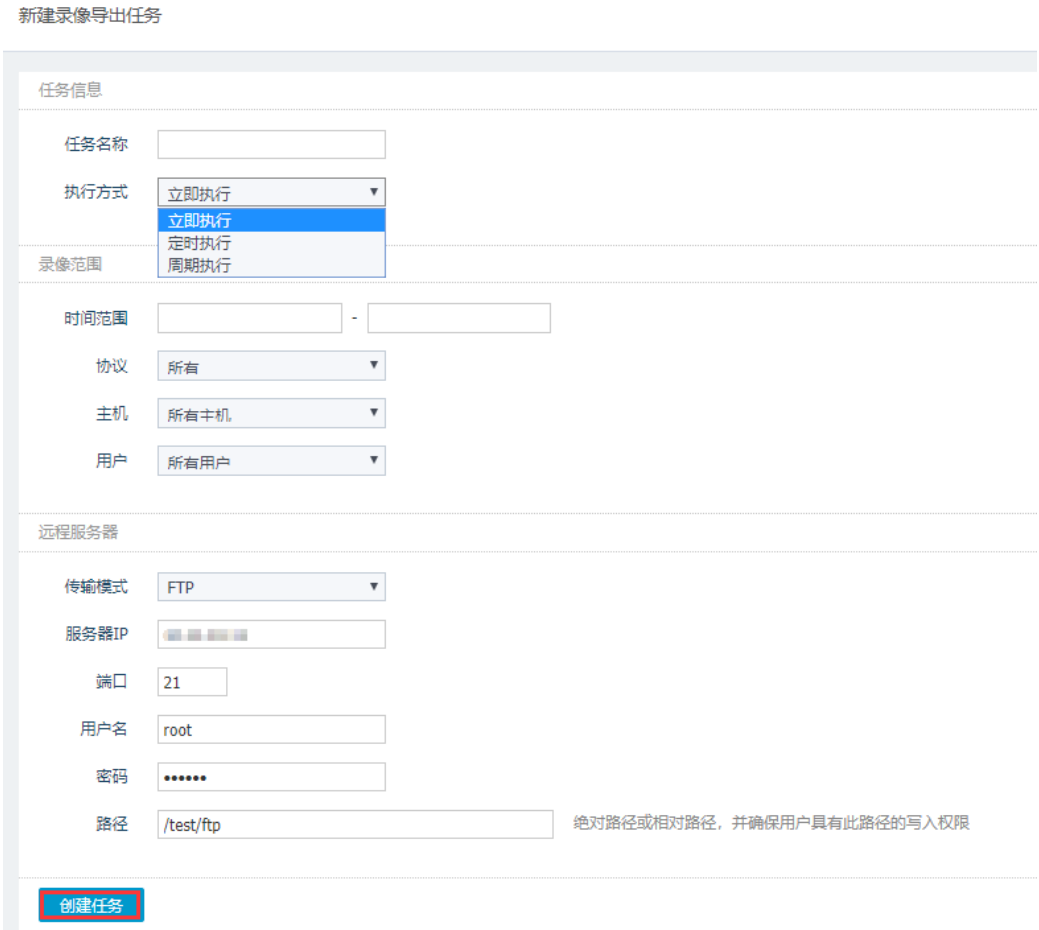
该章节介绍如何将录像导出到本地。

背景信息

通过录像导出任务，把堡垒机中的运维录像保存到远程服务器，方便管理员备份和查看。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 存储管理 > 录像导出**页面。
3. 单击**新建录像导出任务**。
4. 在**新建录像导出任务**页面，设置导出参数。



   - 任务信息：用于设置**任务名称**和**执行方式**，**执行方式**支持*立即执行*、*定时执行*、*周期执行*。

- 录像范围：设置需要导出录像的范围。
- 远程服务器：设置导出录像保存的远程服务器信息。

5. 单击**创建任务**，完成录像导出任务的创建。
6. 手动管理录像导出任务。

   （可选）在任务列表中，勾选需要手动操作的任务，进行开始、暂停、删除等操作。

10.8.6.4.3. 日志备份

该章节介绍如何备份堡垒机日志。

背景信息

日志备份功能可以备份操作日志和会话日志，同时支持下载日志备份保存到本地，方便管理员后续查看日志。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 存储管理 > 日志备份**页面。
3. 在**日志备份**区域，设置需要备份的日志信息。

   可设置需要备份的日志时间段、日志类型等信息。
4. 单击**创建日志备份**，完成日志备份操作。
5. 管理日志备份。

   在**备份列表**区域，下载或删除日志备份。

10.8.6.5. 查看系统操作日志

该章节介绍如何设置操作日志级别和查看操作日志。

操作步骤

1. 使用系统管理员账号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。

   > **说明** 云盾堡垒机系统为每种操作都设置了默认重要性。

   操作日志配置页签



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。

   操作日志页签



> **说明** 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。

10.8.6.6. 查看系统报表

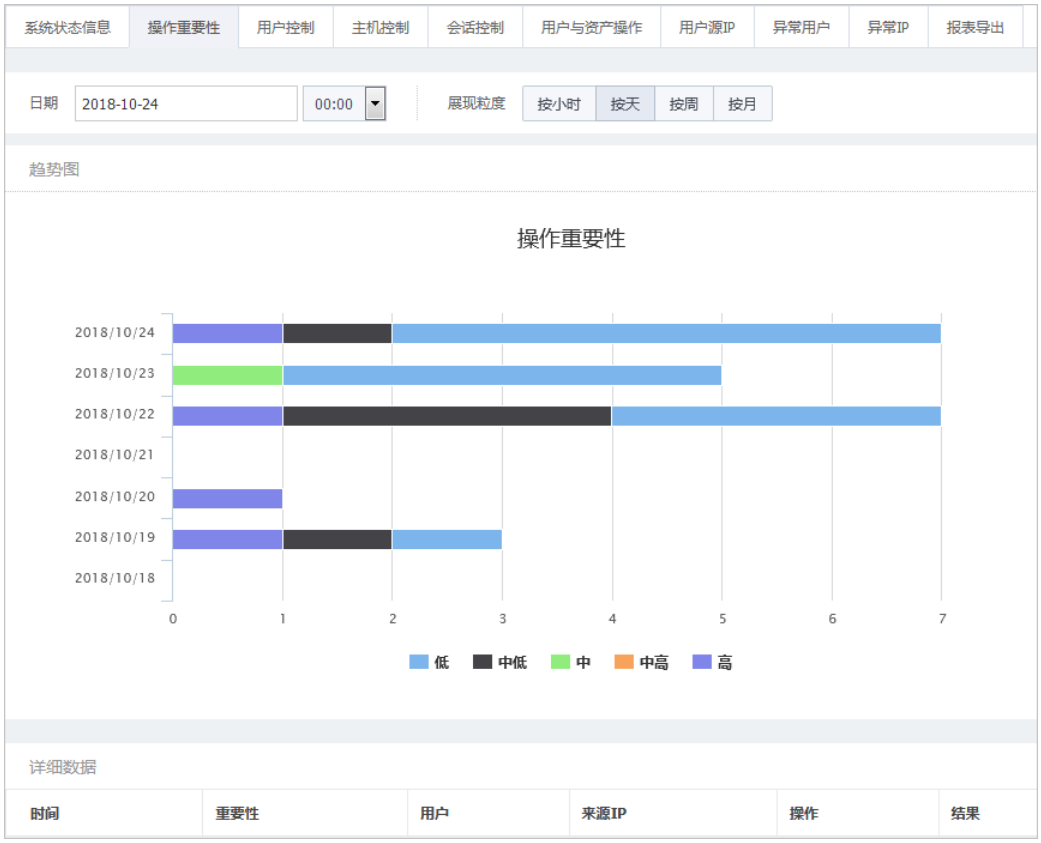
该章节介绍如何查看系统报表。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。

2. 定位到**系统 > 系统报表** 页面。
3. 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。

查看系统报表



系统报表支持查看以下报表：

页签	说明
系统状态信息	查看系统的资源占用情况，包括CPU使用率、内存占用率、系统分区空间使用率和会话分区空间使用率。
操作重要性	查看系统操作的重要性分布情况，重要性分类参考**操作日志**中的**操作日志分类**。
用户控制	查看用户锁定和解锁情况。
主机控制	查看主机禁用和解禁情况。
会话控制	查看会话控制趋势。
用户与资产操作	查看添加和删除的用户数、用户组数、主机数、主机帐户数。
用户源IP	查看源IP数量前五的用户。
异常用户	查看登录系统失败数量前五的用户。
异常IP	查看登录系统失败数量前五的异常IP。

4. 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。

10.8.6.7. 本机维护

10.8.6.7.1. 管理系统

该章节介绍如何设置时间服务器、重启设备、关闭设备、恢复出厂设置等操作。

背景信息

当组网中的时间同步服务器变更后，需要根据该章节修改堡垒机的时间同步服务器。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 系统管理**页面。
3. 在**系统时间**区域，管理系统的时间服务器。

   在**时间服务器**中设置时间同步服务器。
   - 自动同步NTP服务器时间：勾选**自动同步**，系统自动同步NTP时间服务器的时间。
   - 手动同步NTP服务器时间：单击**同步服务器时间**，系统同步NTP时间服务器的时间。
   - 手动同步本地时间：单击**同步浏览器时间**，系统同步浏览器所属本地设备的时间。
4. 在**系统工具**处，进行设备的基本管理操作。
   - 单击**重启设备**，重启堡垒机。
   - 单击**关闭设备**，关闭堡垒机。
   - 单击**恢复出厂设置**，系统恢复为出厂状态。

10.8.6.7.2. 升级系统

该章节介绍如何升级堡垒机系统。

前提条件

已经获取正确的系统升级文件包。

背景信息

通过升级堡垒机的系统版本，使堡垒机运行更加稳定。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护**页面，选择**升级**页签。
3. 在**系统升级**区域，单击**上传系统升级文件**。
4. 在本地选择系统升级文件包并上传。
5. 选择**系统管理**页签，单击**重启设备**。

   重启完成后，系统将升级为新版本。

10.8.6.7.3. 导入许可证

该章节介绍如何导入堡垒机的许可证。

背景信息

堡垒机需要导入许可证才能正常使用。如果您初始导入许可证或到期更换许可证，可以参考本章节内容操作。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 许可证**页面。



3. 申请许可证。
   i. 单击**生成系统认证文件**。
   ii. 将系统认证文件导出后，与相关人员联系并获取许可证文件。
4. 备份许可证。

   获取到有效的许可证文件之后，可将原有的许可证带出到本地备份保存。如果首次导入许可证，可以忽略此步骤。

   i. 单击**备份许可证**。
   ii. 选择本地路径并保存。
5. 导入许可证。

   获取到有效的许可证之后需要将许可证导入系统生效。

   i. 单击**导入许可证**。
   ii. 选择许可证文件并导入。

10.8.6.7.4. 查看资源监控信息

该章节介绍如何查看堡垒机系统资源的实时使用情况。

背景信息

通过资源监视，查看堡垒机的运行情况，当资源占用过高时，根据实际情况判断是运行故障还是需要进行扩容。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 资源监视**页面。
3. 查看CPU、内存、网络、硬盘等资源占用情况。

10.8.6.7.5. 备份还原系统配置

该章节介绍如何备份/还原系统配置。

背景信息

当需要更换设备时，可以先备份原来设备的系统配置，再还原到新设备上，实现快速部署堡垒机。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 系统备份**页面。
3. 备份系统配置。

   系统支持手动备份和自动备份两种方式：

   - 手动备份
     a. 在**系统配置手动备份**区域，编辑备注信息。
     b. 单击**创建系统配置备份**，**备份列表**中即可产生备份信息。
   - 自动备份
     a. 在**系统配置自动备份**区域，**状态**设置为*开启*。
     b. 设置备份的**周期**、**保留备份数**等信息。
     c. 单击**保存更改**。
4. 还原系统配置。

   > **说明** 在备份系统配置前，建议先备份原来的系统配置信息。

   - 在备份列表还原系统配置。
     a. 在**备份列表**中，定位到需要还原的备份信息。
     b. 单击**还原**，将备份的系统配置恢复还原至系统中。
   - 上传备份文件进行还原。
     a. 在**系统配置还原区域**，单击**上传系统配置文件**。
     b. 选择本地的系统配置备份文件，上传并还原至系统中。

5. （可选）其他管理操作。

   除了备份和还原，还支持以下操作：

   - 下载备份
     a. 在**备份列表**中，定位到需要下载的备份信息。
     b. 单击**下载**，将系统配置的备份文件下载到本地。
   - 删除备份
     a. 在**备份列表**中，定位到需要删除的备份信息。
     b. 单击**删除**，删除系统配置的备份信息。

10.8.6.7.6. 推送和接收系统配置

该章节介绍如何对系统配置进行同步推送和接收。

背景信息

开启系统配置推送，系统将按照设定的推送周期向目标设备推送本设备的系统配置。通过系统同步推送和接收功能，其他堡垒机能够快速同步本堡垒机的系统配置信息，达到批量部署的目的。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护**页面。
3. 配置一台堡垒机作为系统同步推送端。
   i. 选择**系统同步推送**页签。
   ii. 在**系统同步推送**区域，开启推送功能，单击**保存更改**。

配置项	说明
状态	设置为*开启*。
推送周期	设置推送的时间周期。
推送密钥	设置推送认证时的密钥。

   iii. 在**添加推送目标**区域，设置推送目标，单击**添加目标**。

配置项	说明
名称	设置推送目标名称。
目标IP	设置推送目标的IP。
Web端口	设置推送目标的Web端口。

   iv. 在**目标推送列表**中，可以查看、手动推送、删除推送目标。
4. 配置其他堡垒机作为推送接收端。
   i. 登录其他堡垒机。
   ii. 选择**系统 > 本机维护 > 系统同步接收**。

iii. 在**系统配置接收**区域，开启接收功能，单击**保存更改**。

配置项	说明
状态	设置为*开启*。
源设备密钥	输入源设置的**系统同步推送**中设置的**推送密钥**。

推送成功后，可以在**接收结果**页面查看上次接收的时间、结果等信息。

10.8.6.7.7. 查看调试日志

该章节介绍如何查看调试日志。

背景信息

堡垒机运行出故障等问题时，可以通过查看调试日志，定位问题根因。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 调试日志**页面。
   在该页面可以查看系统的调试日志。
3. 单击**关闭刷新**，暂停调试日志的更新。
4. 单击**导出日志**，将调试日志导出到本地查看。

10.8.6.7.8. 网络诊断

该章节介绍如何使用网络诊断工具检查网络的连通性。

背景信息

通过网络诊断，判断主机的IP或端口是否连通、路由是否可达、TCP端口是否连通、UDP端口是否连通。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 网络诊断工具**页面。
3. 在**连通性检测**区域，设置检测类型。
   检测主机的IP或端口是否连通、路由是否可达、TCP端口是否连通、UDP端口是否连通。
4. 单击**执行测试**，自动检测并返回检测结果。

10.8.6.7.9. 系统诊断

该章节介绍如何通过系统诊断工具进行系统诊断。

背景信息

通过系统诊断，判断堡垒机的系统、内存、磁盘等信息，为设备运维、排查故障提供帮助。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 系统诊断工具**页面。
3. 查看系统各设备信息和前十个进程。
4. 单击**下载诊断日志**，将诊断日志下载到本地查看。

10.8.6.7.10. 查看系统警报

该章节介绍如何查看系统警报。

背景信息

产生系统警报后，管理员可在此页面查看并确认系统警报。CPU、内存、网卡等状态检测周期为5分钟。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 系统警报**页面。
3. 查看系统警报列表，根据警报判断是否需要进行故障排查。
4. 完成故障排查后，勾选警报，单击**确认警报**。

10.8.6.7.11. 生成控制台SSH公钥

该章节介绍如何生成控制台SSH公钥。

背景信息

控制台SSH公钥适用于需要登录堡垒机后台但忘记了root密码时的场景。重置控制台SSH公钥会自动重新生成一对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，请妥善保管好私钥。

操作步骤

1. 使用系统管理员账号登录云盾堡垒机系统。
2. 定位到**系统 > 本机维护 > 控制台SSH公钥**页面。
3. 单击**重置控制台SSH公钥**。
4. 单击**确定**，完成控制台SSH公钥的重置。

> **说明** 控制台SSH公钥重置后会弹出窗口显示私钥，请及时保存并妥善保管私钥，窗口关闭后若遗忘私钥，只有通过重置生成新的私钥！

后续步骤

通过SSH私钥，可以使用SSH工具登录堡垒机。

10.9. 堡垒机（New）

10.9.1. 创建和登录堡垒机

本文介绍如何创建并登录堡垒机。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云原生堡垒机**。
3. 在页面右上角，单击**创建实例**。
4. （可选）如果用户所在的组织没有堡垒机的RAM角色，需要根据提示为组织创建堡垒机的RAM角色。



   i. 在提示框中，单击**去授权**。
   ii. 在**组织**中选择用户所在组织，在**服务**中选择**堡垒机**。



   iii. 单击**确定**，完成创建堡垒机RAM角色的操作。
5. 在**VPC ID**和**Vswitch ID**中分别选择堡垒机所在的VPC和交换机，并设置**资产上限**。

> **说明** 创建堡垒机实例时，您可以设置当前堡垒机实例支持托管的资产上限数量。所有堡垒机实例支持托管的总资产数量取决于您购买的堡垒机授权（license）数量。如果需要增加授权数量，您可以联系销售反馈您的需求。



6. 单击**确定**，系统开始创建堡垒机。
   系统创建堡垒机需要一些时间，当堡垒机的**状态**为**正常**，**集群状态**为**已创建**时，表示堡垒机创建成功。
7. 创建成功后，单击堡垒机的**详情**，进入堡垒机环境。

10.9.2. 管理员操作指南

10.9.2.1. 系统管理

10.9.2.1.1. 设置Web登录超时时间

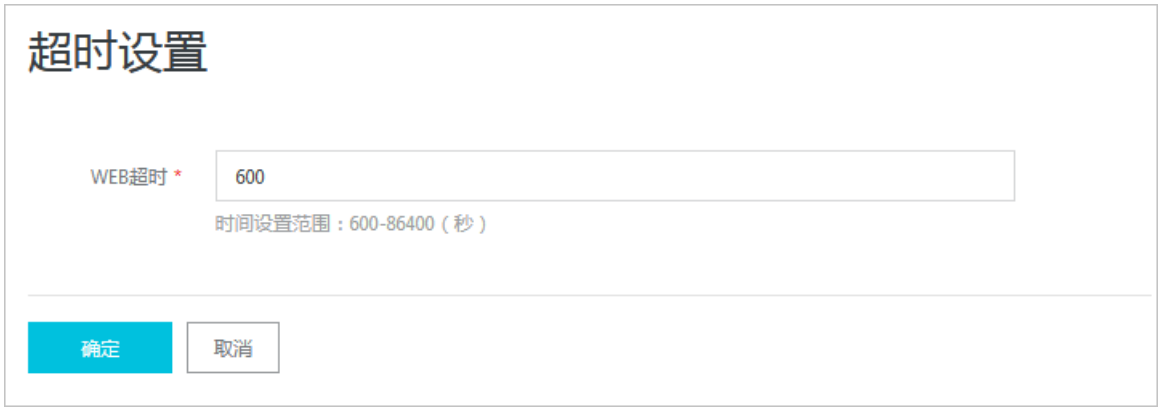
本文介绍如何设置用户登录堡垒机Web页面的超时时间。

背景信息

如果您登录堡垒机的Web管理页面后，在超时时间内没有任何操作，您的账号将自动退出。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**安全 > 全局平台安全 > 云原生堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航树选择**系统管理**，在**系统管理**页面单击**超时设置**。
4. 在**超时设置**页面，输入**WEB超时**的时间，单击**确定**。



10.9.2.1.2. 设置对外输出方式

该章节介绍堡垒机的对外输出方式，支持邮件、短信网关和FTP等模式。

设置邮件

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**系统管理 > 输出设置**。
4. 选择**邮件**页签。
5. 单击**创建**。
6. 在**新增邮件配置**对话框中，设置邮件发送信息。



参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
服务器地址	发送邮件服务器地址。
端口	发送邮件服务器端口。
连接方式	支持的连接方式包括*加密*和*非加密*。
发送邮箱地址	发送邮件的邮箱账号。
服务器账号	账号信息。
服务器验证	邮箱账号登录是否需要验证。
附件大小	邮件发送附件的最大值。
编码方式	邮件服务器编码格式，支持*UTF-8*和*GBK*。
方式	配置该邮件服务器为默认发送服务器或备用发送服务器。

参数	说明
测试	测试邮件服务器是否能够正常发送。 在输入框中输入接收邮箱账号，单击**测试**。

7. 单击**保存**。

设置短信网关

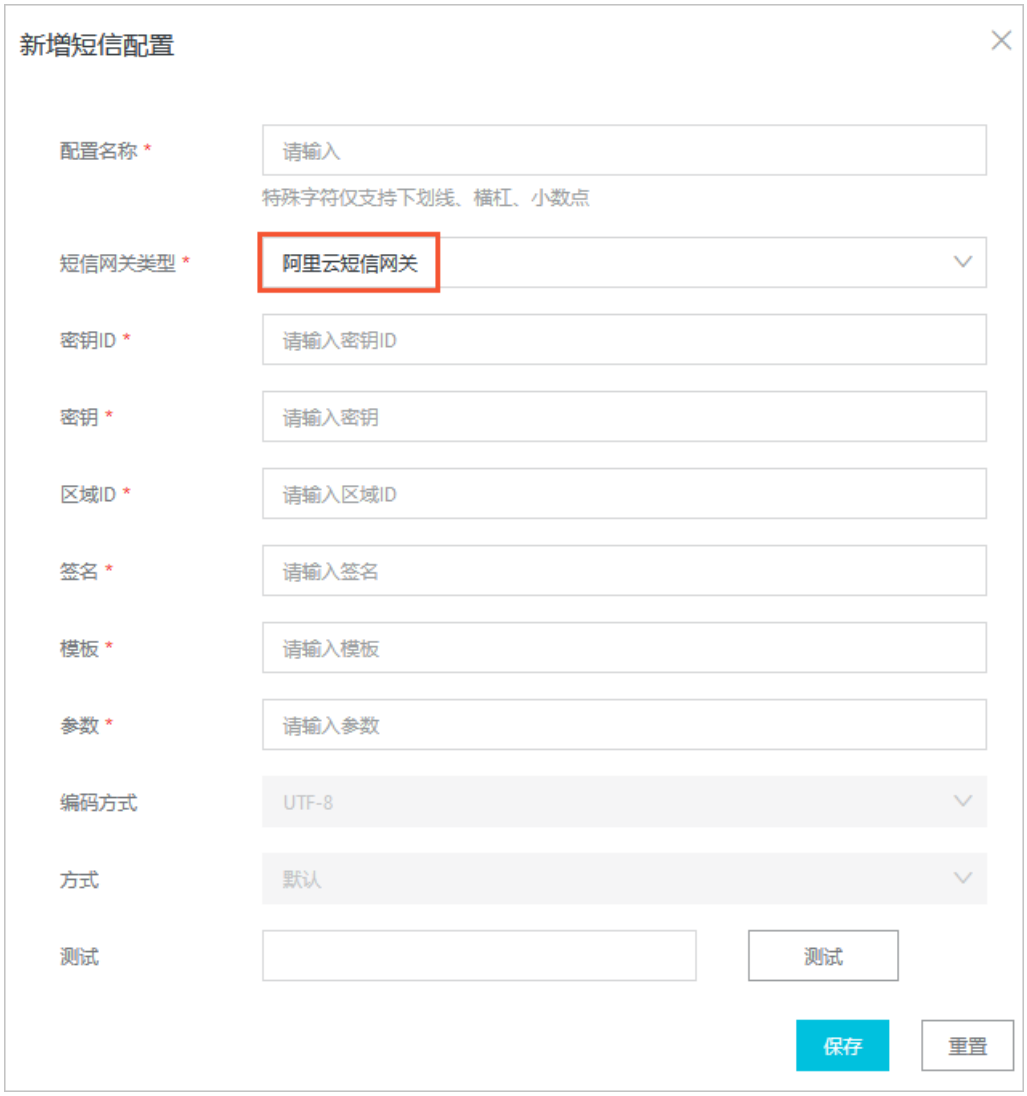
1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**系统管理 > 输出设置**。
4. 选择**短信网关**页签。
5. 单击**创建**。
6. 在**新增短信配置**对话框中，设置短信网关参数。根据短信网关的类型，支持配置**数据库短信网关**和**阿里云短信网关**。
   - 数据库短信网关



参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
短信网关类型	在下拉框中选择*数据库短信网关*。
数据库类型	在下拉框中选择数据库类型，支持*ORACLE*、*MSSQL*、*MYSQL*和*SYBASE*。
服务器地址	填写数据库服务器地址。
端口	填写数据库服务器端口。
账号	填写数据库账号
密码	填写数据库密码。
数据库	填写数据库名。

参数	说明
短信sql语句模板	插入的SQL语句模板。
编码方式	短信内容的编码格式，支持*UTF-8*和*GBK*。
方式	配置该服务器为默认发送服务器或备用发送服务器。
测试	测试服务器是否能够正常发送。

- 阿里云短信网关



参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
短信网关类型	在下拉框中选择*阿里云短信网关*。
密钥ID	填写账号密钥ID。

参数	说明
密钥	填写账号密钥。
区域ID	填写区域ID。
签名	填写短信签名。
模板	填写短信模板ID。
参数	填写短信模板中用到的模板变量名称。
编码方式	短信内容的编码格式，支持*UTF-8*。
方式	配置该服务器为默认发送服务器或备用发送服务器。
测试	测试服务器是否能够正常发送。

7. 单击**保存**。

设置FTP

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**系统管理 > 输出设置**。
4. 选择**FTP**页签。
5. 单击**创建**。
6. 在**新增FTP配置**对话框中，设置FTP参数。



参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
服务器地址	填写FTP服务器地址。
端口	填写FTP服务器端口。
用户名	填写FTP账号。
用户密码	填写FTP密码。
上传路径	填写上传FTP的指定文件夹路径。
方式	配置该服务器为默认发送服务器或备用发送服务器。
模式	FTP的传输模式，支持*被动*和*主动*。

7. 单击**保存**。

10.9.2.2. 用户管理

10.9.2.2.1. 配置全局安全策略

配置堡垒机的全局安全策略。安全策略保障用户账号的安全性。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航树，选择**运维管理 > 授权管理**，单击**全局策略**。
4. 选择**安全策略**页签，设置全局安全策略，单击**保存**。



设置项	说明
密码最小长度	设置堡垒机用户登录密码位数，最小为6位，最大为32位，缺省为8位。
密码使用期限	设置密码有效期，用户在密码到期前必须修改密码。 系统可设置密码过期提示天数，在密码过期前提示用户修改密码，0表示不提示。
密码复杂程度要求	设置密码必须包含哪类字符。
密码安全策略	设置密码不允许重复使用的次数。
账户锁定策略	设置账号锁定策略及账号锁定后的自动解锁时间。
登录验证码	启用登录验证码后，用户登录时需要输入图片验证码。

10.9.2.2.2. 配置用户认证模式

用户登录堡垒机时需要登录认证，用于提高堡垒机的安全。该章节介绍如何配置认证模式和新增认证模块。

配置认证模式

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航树，选择**运维管理 > 运维管理**，单击**认证模块**。

4. 单击**创建**。
5. 设置用户登录的认证方式，单击**保存**。



设置项	说明
名称	输入认证方式的名称。
默认	启用后，该认证方式将作为创建用户时的默认认证方式。
验证方式	选择验证方式。 ○ **全部通过**：表示需要符合所有认证模块才能认证通过。 ○ **任一通过**：表示只需要符合一项认证模块，即可认证通过。
模块配置	在下拉栏中选择认证模块。 通过单击+，可以设置多个认证模块。 **说明** 如果需要添加更多认证模块，通过单击**模块管理**进行操作，具体步骤参见添加认证模块。

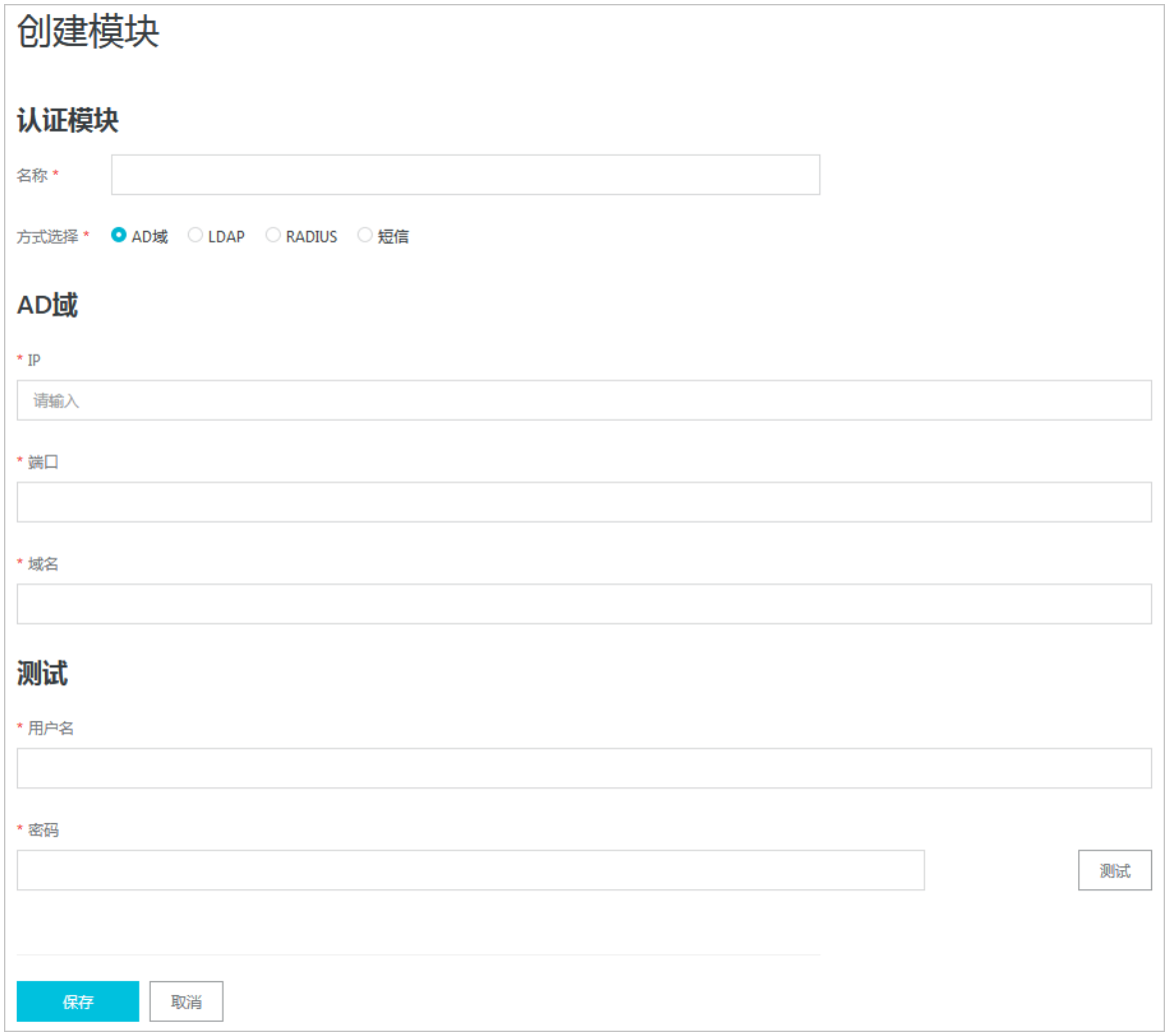
添加认证模块

此处以添加**AD**认证为例进行介绍，具体步骤如下：

说明 AD（Active Directory）存储有关网络上对象的信息，并使管理员和用户可以轻松查找和使用此信息。此处AD认证使用Microsoft AD域帐号进行身份认证。

1. 在**创建认证方式**对话框，单击**模块管理**。

   进入**创建认证方式**对话框的具体步骤参见配置认证模式。
2. 单击**创建**。
3. 在**认证模块**区域，设置认证模块名称和选择认证方式。



配置项	说明
名称	输入认证模块名称。
方式选择	选择认证方式，支持**AD域**、LDAP、RADIUS和**短信**。 此步骤以选择**AD域**为例。

4. 在**AD域**区域，输入AD域的服务器信息。

> **说明** AD域服务（Active Directory Domain Service，AD DS），负责AD目录数据库的存储、添加、删除、修改与查询等操作。

配置项	说明
IP	输入AD域的服务器IP。
端口	输入AD域的服务器端口号。
域名	输入AD域的服务器域名。

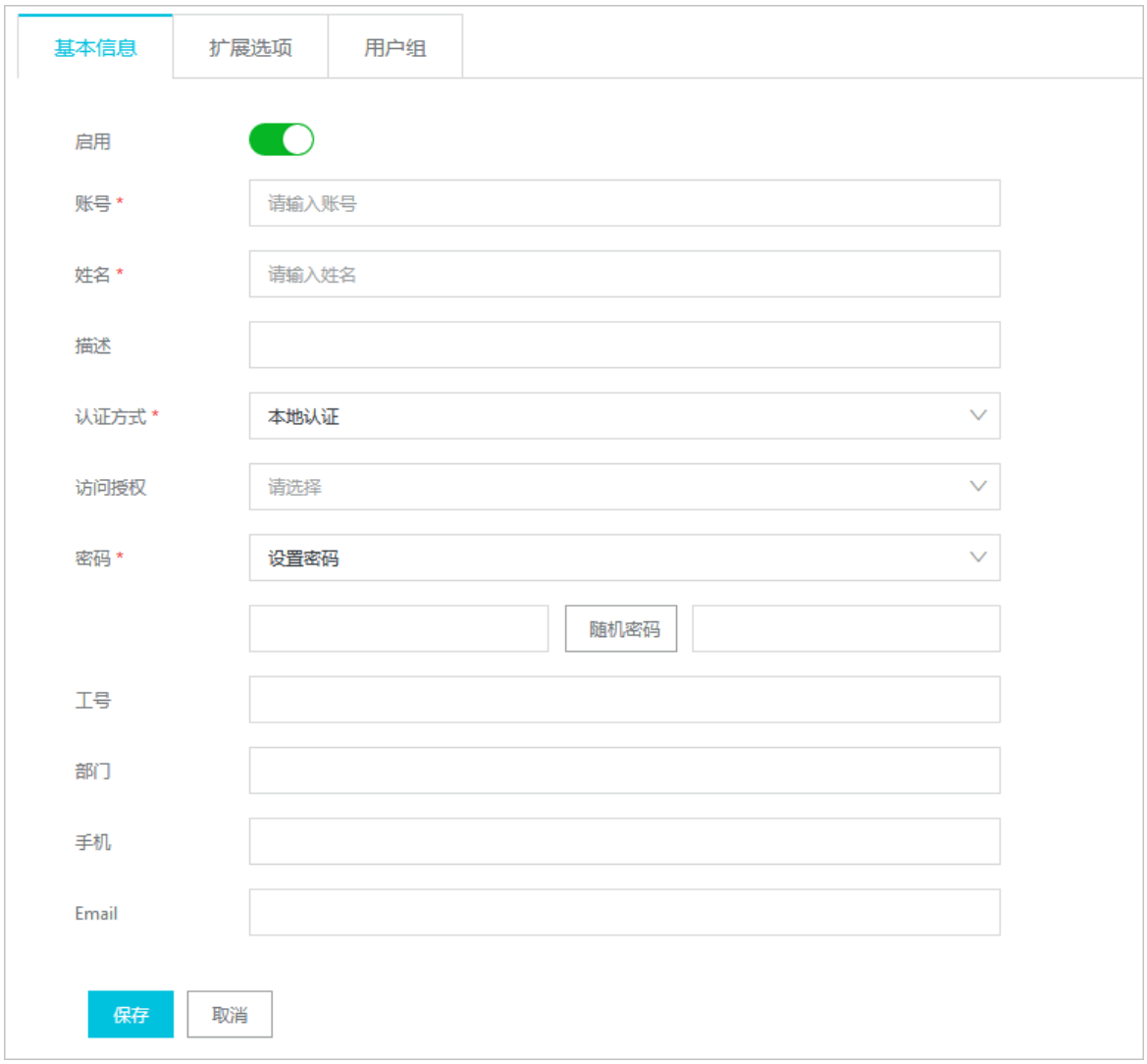
5. 在**测试**区域，输入**用户名**和**密码**，单击**测试**，测试堡垒机和AD域服务器的连通性。
6. 测试成功后，单击**保存**，完成创建认证模块操作。

10.9.2.2.3. 创建用户

本文介绍如何在堡垒机中为运维和审计人员创建用户账号。一个用户账号应该只和一个责任人对应，方便管理和后期的问题回溯。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏，选择**运维管理 > 运维管理**，单击**系统用户**。
4. 选择**基本信息**页签，设置用户参数。



设置项	说明

设置项	说明
启用	启用用户开关。 ○ 在启用状态时，创建完用户就可以直接使用。 ○ 在关闭状态时，创建完用户不能直接使用，需要启用后才能使用。
账号	用户的账号名称。
姓名	用户所属的运维人员姓名。
描述	输入该用户的备注内容，便于您后续查看和管理用户。
认证方式	选择用户登录时的认证方式。缺省为本地认证方式，也可以指定用户采用其他已配置的认证方式。 认证方式的配置方法，具体参见配置用户认证模式。
访问授权	选择访问授权方式。
密码	设置用户的密码，可选择**初始密码**或**设置密码**。您可以输入密码，也可以单击**随机密码**生成密码。
工号	运维人员的工号。
部门	运维人员的部门。
手机	运维人员的手机号码。
Email	运维人员的Email地址。

5. 选择**扩展选项**页签，设置用户的扩展功能。



设置项	说明
第三方认证账号	当采用第三方认证方式时，绑定其第三方认证服务器上的账号名称。
唯一登录	启用后，将限制账号在同一时间内只能在一个IP地址登录。

设置项	说明
失效时间	启用后，到达指定的失效时间后账号将自动停用。

6. 选择**用户组**页签，设置用户所属的用户组。

> **说明** 如果未选择用户组，该用户将属于**未分组**。



7. 单击**保存**，创建新用户。

10.9.2.2.4. 创建用户组

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. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在**运维管理**页面，单击**用户管理**。
4. 单击**创建用户组**。



5. 设置用户组的**名称**、**描述**和**访问授权**等信息。



6. 单击**保存**，完成创建用户组操作。

10.9.2.3. 主机管理

10.9.2.3.1. 创建主机账号

本文介绍如何在堡垒机中创建运维主机的账号。

背景信息

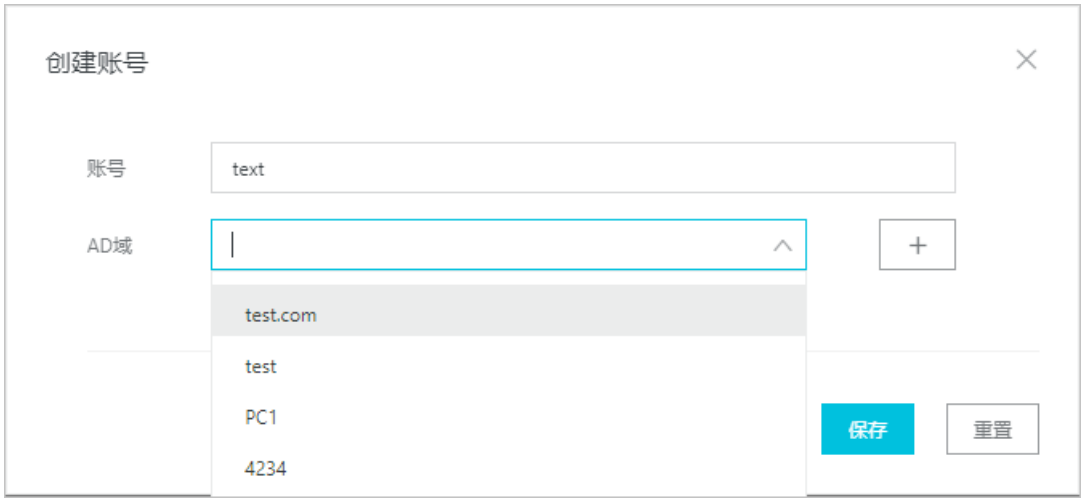
堡垒机已经存在部分默认的主机账号，部分默认账号的信息说明如下：

- *****：任意账号，允许用户在登录时自行填写。
- **-**：空账号，有密码但账号名为空，一般交换机中会出现。
- **#**：单点登录账号，与堡垒机登录的运维账号相同。

如果默认账号不能满足您的需求，您可以参照本章节创建新的主机账号。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在**运维管理**页签下，单击**主机账号**。
4. 单击**创建**。
5. 输入账号信息，单击**保存**。



设置项	说明
账号	输入账号名称。
AD域	可选项，选择账号的AD域服务器。

如果您需要同时添加多个账号，输入**账号**和选择**AD域**后，单击 + 图标，重新添加新的账号信息。

10.9.2.3.2. 创建主机的设备类型

本文介绍如何为堡垒机添加新的设备类型。

背景信息

堡垒机默认已经提供部分常用的主机设备类型，如果您的设备不在这个范围内，可以通过本文自己创建新的设备类型。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**运维管理**，单击**设备类型**。
4. 单击**创建**。
5. 在**创建设备类型**对话框中，配置设备类型，单击**保存**。



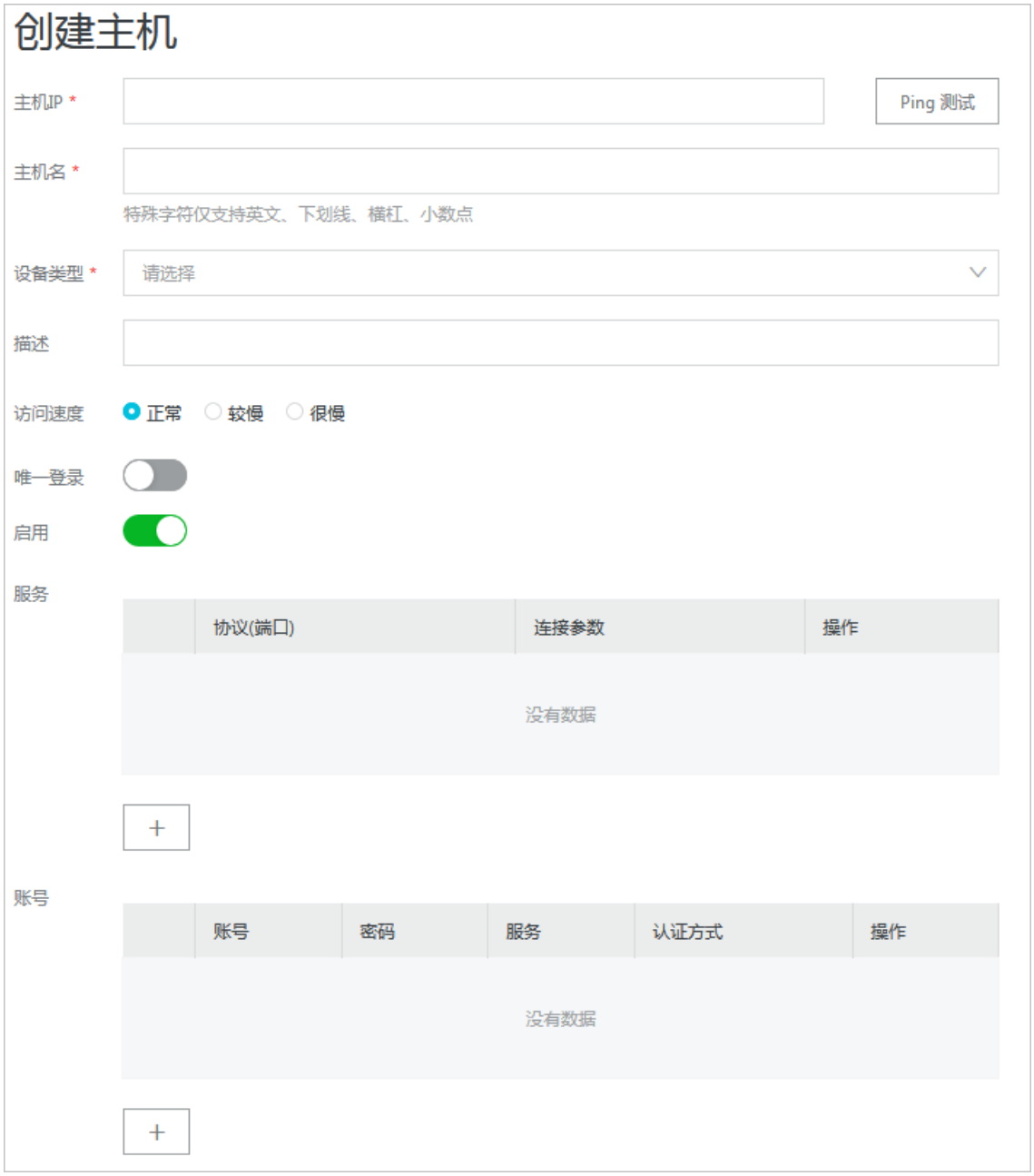
配置项	说明
请选择	选择堡垒机支持的设备类型。
名称	输入设备名称。
账号切换命令	设备切换登录账号时使用的命令。
密码切换提示	设备切换登录账号时的密码提示符。
描述	输入设备的详细注释。
隐藏	是否隐藏该设备类型，隐藏后在创建主机过程中配置主机类型时将不能选择该设备类型。
配置服务	单击加号图标，选择主机的服务协议类型和端口号。

10.9.2.3.3. 手动创建主机

本文介绍如何在堡垒机中手动创建需要通过堡垒机运维的主机。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航树选择**运维管理**，在**运维管理**页签单击**主机**。
4. 在**创建主机**页面，设置主机参数。



设置项	说明
主机IP	输入主机的IP地址。 单击**Ping测试**，可以测试堡垒机和该主机之间的网络是否连通。
主机名	输入主机名称。 特殊字符仅支持英文、下划线（_）、短划线（-）、半角句号（.） 。

设置项	说明
设备类型	在下拉框中选择设备的类型，可选择类型包括**Windows**、**Linux**、**Unix**等操作系统；**Cisco**、**Huawei**等各厂商硬件。
描述	输入该主机的备注内容，便于您后续查看和管理主机。
访问速度	选择访问速度，可选择**正常**、**较慢**或**很慢**。
唯一登录	启用后，该主机同一时间只允许一个用户连接。
启用	启用该主机。 ○ 在启用状态时，用户可以运维该主机。 ○ 在关闭状态时，用户不可以运维该主机，需要先启用该主机才能运维。
服务	单击 + 图标，设置需要运维的主机服务。 例如：主机为Linux，可以设置SSH、FTP、数据库等服务。
账号	单击 + 图标，设置需要运维的主机账号。 在堡垒机中创建主机账号的操作步骤，请参见创建主机账号。
主机组	选中主机所属的主机组。

5. 单击**保存**，完成手动创建单个主机操作。

10.9.2.3.4. 批量导入主机

除了手动创建主机，您也可以批量导入同一VPC下所有的主机。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在**运维管理**也签下，单击**主机管理**。
4. 单击**主机导入**。



5. 在下拉栏中选择**VPC**，单击**保存**，批量导入主机。



> **说明** 如果启用**覆盖相同IP的主机**，则如果导入主机中IP和已创建的主机IP相同，新导入的主机信息会覆盖原来已创建的主机信息。

10.9.2.3.5. 创建主机组

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. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在**运维管理**页签下，单击**主机管理**。
4. 单击**创建主机组**。



5. 设置主机组的**组名**和**描述**等信息。



6. 单击**保存**，完成创建主机组操作。

10.9.2.4. 运维管理

10.9.2.4.1. 配置全局运维策略

配置堡垒机的全局运维策略，全局运维策略的优先级高于访问授权策略中的权限配置。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏单击**运维管理**，在**授权管理**页签单击**全局策略**。
4. 选择**运维策略**页签，设置全局运维策略，单击**保存**。



设置项	说明
代填分隔符	仅支持and（&）、竖线（|）、at（@）。
超时设置	启用并设置阈值后，运维会话如果在该时间内无操作将断开连接。
运维访问通道	启用后所有运维访问会话都会通过运维访问通道进行连接，客户端与堡垒机运维访问通道端口必须保证通信正常，端口缺省为8088。
文件传输记录	启用后可在**访问授权**中配置文件记录权限，并设置传输文件记录保存的最大存储空间。
隐藏主机IP	启用后运维用户界面无法查看主机IP。

设置项	说明
账号密码保存	选择运维访问时是否保存主机账号/密码，可选值：**提示**、**保存**、**不保存**。
应用发布访问控制	启用后应用发布不允许访问除目标主机外的其他IP。
登录审批	启用后所有运维会话访问都需要通过管理员审批。 启用审批时可以应用已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。
访问备注	启用后所有运维会话访问都需要填写操作备注。
协同登录	启用后所有运维会话访问都需要邀请任意其他运维用户共同操作会话。
登录告警	选择登录告警策略，可选值：**不告警**、**登录告警**。 选择告警时可以应用已设置好的事件告警。如果没有可选择的事件告警，可以从下拉栏中单击**新增**，新增事件告警。新增事件告警的操作请参见创建事件告警。
指定应用发布	配置应用发布为**内置**或**外置**，以及外置应用发布服务器IP。

10.9.2.4.2. 配置访问授权

本文介绍如何配置用户与主机之间的访问关系及运维权限。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏选择**运维管理**，在**资产管理**的**运维管理**页签下，单击**授权管理**。
4. 在**授权管理**页面的**访问授权**页签，单击**创建**。
5. 在**运维用户**中选择用户等信息，单击**下一步**。

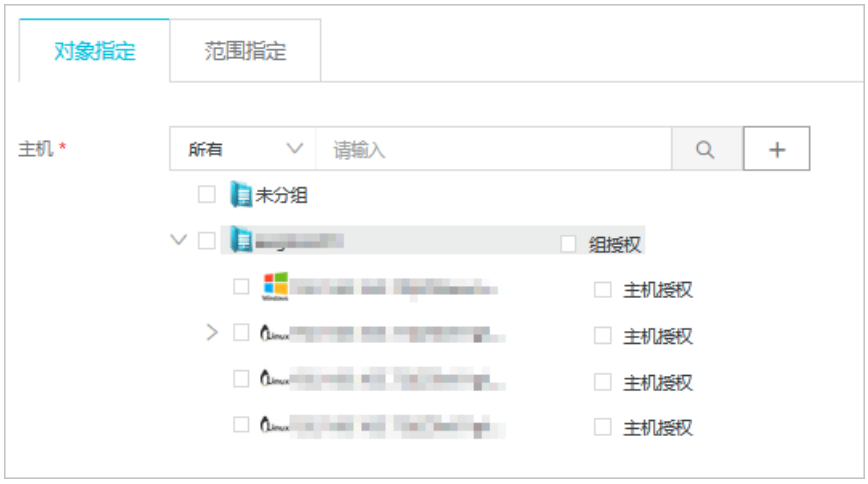


设置项	说明
授权名称	输入访问授权策略的名称。
是否启用	设置该访问授权策略是否启用。
授权动作	设置访问授权的授权动作，可选**允许**或**拒绝**。 ○ **允许**：表示访问授权策略中的用户允许访问目标主机。 ○ **拒绝**：表示访问授权策略中的用户禁止访问目标主机。
用户	选择访问授权策略生效的用户。 ○ 选中**组授权**，表示此访问授权策略对该组中所有用户都生效。 ○ 选中部分用户，表示此访问授权策略对已选择的用户生效。

6. 在**访问范围**中选择访问目标，单击**下一步**。

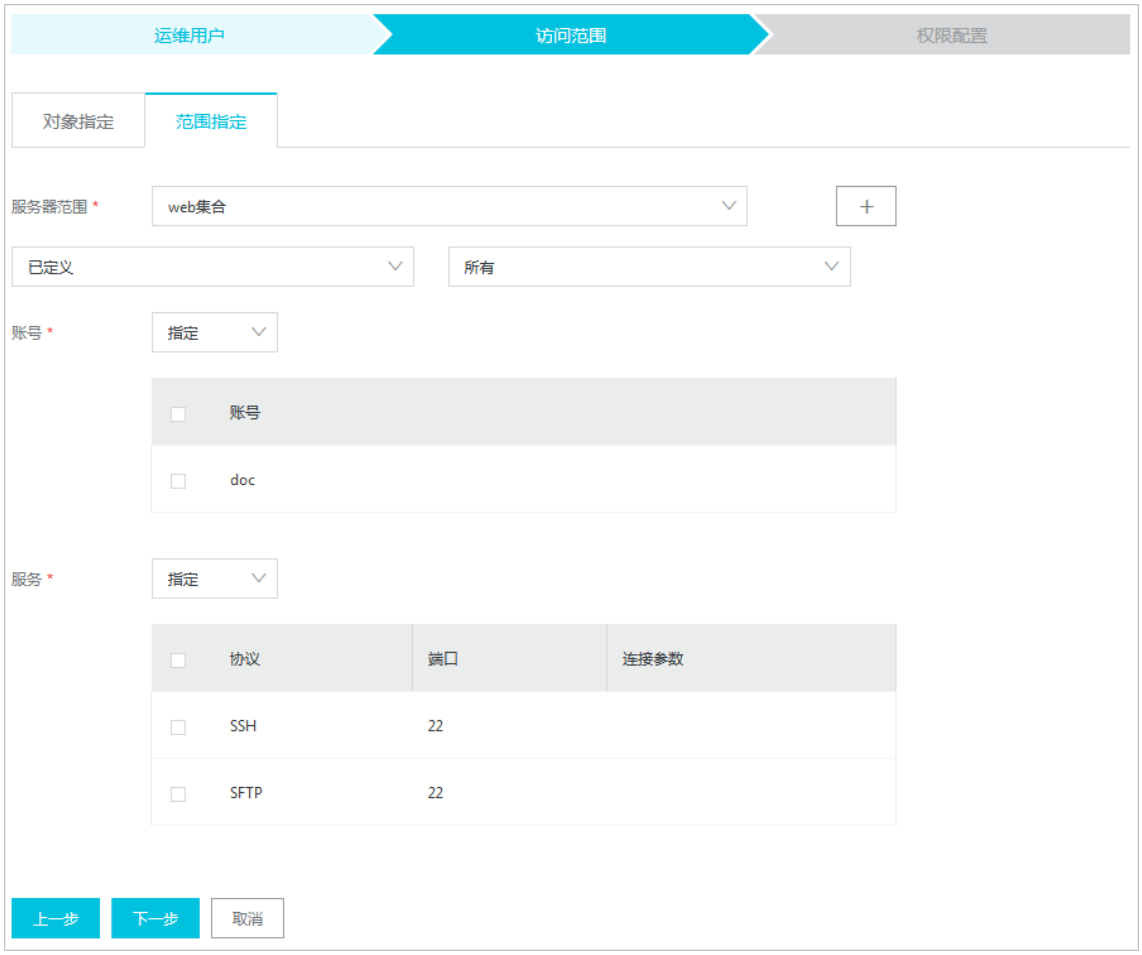
   访问目标可选择指定的具体服务、主机或主机组；也可以选择一定范围内的所有主机。

   ○ 选中**对象指定**页签，选择指定的具体服务、主机或主机组。



- 选中**组授权**：表示此访问授权策略对该组中所有主机都生效。
- 选中**主机授权**：表示此访问授权策略对该主机中所有服务都生效。
- 选中具体服务：表示此访问授权策略对选中的服务生效。

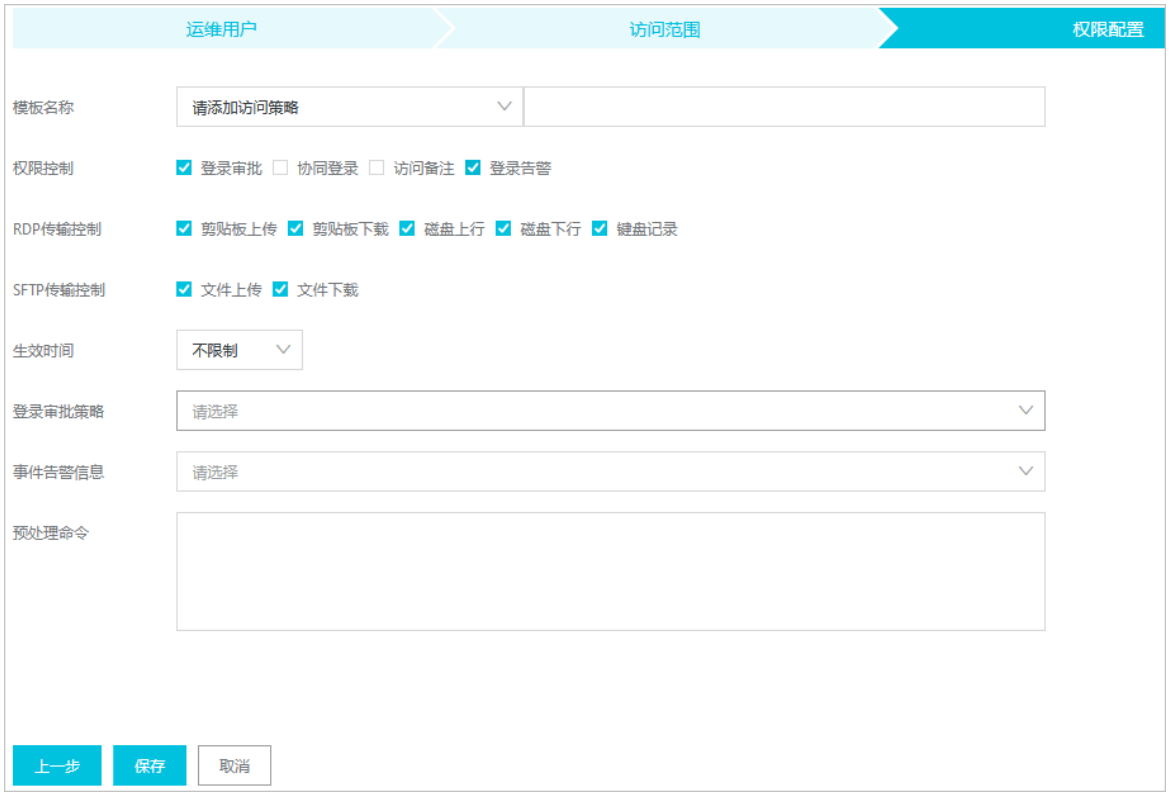
○ 单击**范围指定**页签，选择一定范围内的所有主机。



设置项	说明
服务器范围	在下拉栏中选择服务器合集，单击 + 图标可以选择多个服务器合集。

设置项	说明
账号范围	选择访问服务器合集的账号范围。 ■ 选择**已定义**，表示您在**账号**中只能选择服务器合集中的主机关联的账号。 ■ 选择**自定义**，表示您在**账号**中可以选择堡垒机中创建的所有账号。
账号	选择访问服务器合集中主机所使用的账号。 ■ **所有**：**账号范围**限定内的所有账号。 ■ **指定**：选择具体账号。
服务	单击 + 图标，设置需要运维的主机服务。 ■ **所有**：**服务器范围**中所有的服务类型。 ■ **指定**：选择服务类型。

7. 在**权限配置**中，设置访问授权的权限限制条件，单击**保存**。



设置项	说明
模板名称	在下拉栏中选择已配置模板，或在下拉栏中单击**新增**，输入模板名称，创建新的模板。

设置项	说明
权限控制	选择用户登录主机时的权限控制策略。 ○ **登录审批**：用户每次访问主机时都需要经过管理员审批。 ○ **协同登录**：用户每次访问主机时需要邀请任意其他用户共同操作会话。 ○ **访问备注**：用户每次访问主机时需要填写访问主机的备注信息。 ○ **登录告警**：用户每次访问主机时触发登录告警。
RDP传输控制	使用RDP远程访问桌面服务时，是否允许**剪贴板上传**、**剪贴板下载**、**磁盘上行**、**磁盘下行**或**键盘记录**等操作。
SFTP传输控制	使用SFTP服务时，是否允许**文件上传**或**文件下载**操作。
FTP传输控制	使用FTP服务时，是否允许**文件上传**或**文件下载**操作。
生效时间	设置访问授权策略的有效时间范围。 ○ **不限制**：表示访问授权设置完成并启用后，该策略一直有效。 ○ **允许**：表示访问授权策略在允许的时间范围内，该策略有效。 ○ **例外**：表示访问授权策略在例外的时间范围内，该策略无效；在其他时间范围内，该策略生效。
登录审批策略	可选，只有**权限控制**包含**登录审批**时需要设置。 从下拉栏中选择已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。
事件告警信息	可选，只有**权限控制**包含**登录告警**时需要设置。 从下拉栏中选择已设置好的事件告警。如果没有可选择的事件告警，可以从下拉栏中单击**新增**，新增事件告警。新增事件告警的操作请参见创建事件告警。
预处理命令	运维用户每次连接主机后会自动执行该命令，仅限字符型会话（例如SSH），多个命令可用英文半角分号（;）分隔。

10.9.2.4.3. 配置指令授权（按对象授权）

指令授权是指允许或拒绝选定的用户在目标主机上执行某些命令。按对象授权的方式，表示您需要自己设定用户和目标主机。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏选择**运维管理**，在**资产管理**页面的**授权管理**页签，单击**按对象授权**。
4. 在**运维用户**中选择用户等信息，单击**下一步**。



设置项	说明
授权名称	输入指令授权策略的名称。
是否启用	设置该指令授权策略是否启用。
用户	选择指令授权策略生效的用户。 ○ 选中**组授权**，表示此指令授权策略对该组中所有用户都生效。 ○ 选中部分用户，表示此指令授权策略对已选择的用户生效。

5. 在**访问范围**中选择访问目标，单击**下一步**。

   访问目标可选择指定的具体服务、主机或主机组；也可以选择一定范围内的所有主机。

   ○ 选择**对象指定**页签，选择指定的具体服务、主机或主机组。



   ■ 选中**组授权**：表示此指令授权策略对该组中所有主机都生效。

   ■ 选中**主机授权**：表示此指令授权策略对该主机中所有服务都生效。

   ■ 选中具体服务：表示此指令授权策略对选中的服务生效。

   ○ 单击**范围指定**页签，选择一定范围内的所有主机。



设置项	说明
服务器范围	在下拉栏中选择服务器合集，单击+图标可以选择多个服务器合集。
账号范围	选择访问服务器合集的账号范围。 ■ 选择**已定义**，表示您在**账号**中只能选择服务器合集中的主机关联的账号。 ■ 选择**自定义**，表示您在**账号**中可以选择堡垒机中创建的所有账号。
账号	选择访问服务器合集中主机所使用的账号。 ■ **所有**：**账号范围**限定内的所有账号。 ■ **指定**：选择具体账号。
服务	选择需要运维的主机服务。 ■ **所有**：**服务器范围**中所有的服务类型。 ■ **指定**：选择服务类型。

6. 在**指令集合/响应方式**中，设置指令授权的指令和响应方式，单击**保存**。



设置项	说明
配置指令集合	可配置允许或禁止使用以下指令（指令集）。
手工输入指令	可手工输入指令，多个指令请使用换行符分隔。
指令集合	在下拉栏中选择已设置好的指令集合。
响应方式	如果符合该指令规则，堡垒机的响应方式。 ○ **产生告警**：当触发该指令策略时堡垒机会生成告警事件。 ○ **阻断会话**：当触发该指令策略时堡垒机会将该会话连接中断。 ○ **忽略指令**：当触发该指令策略时堡垒机会将该指令忽略，不执行此命令并提示该指令未找到，会话可继续正常操作。 ○ **审批指令**：当触发该指令策略时会话会暂停等待管理员审批，管理员审批通过后指令会执行并可继续进行其他操作，如果管理员拒绝则指令不会执行但可以继续进行其他操作。
审批策略	可选，只有**响应方式**包含**审批指令**时需要设置。 从下拉栏中选择已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。
告警信息	可选，只有**响应方式**包含**产生告警**时需要设置。 从下拉栏中选择已设置好的告警事件。如果没有可选择的告警事件，可以从下拉栏中单击**新增**，新增告警事件。新增告警事件的操作请参见创建事件告警。

10.9.2.4.4. 配置指令授权（按访问授权）

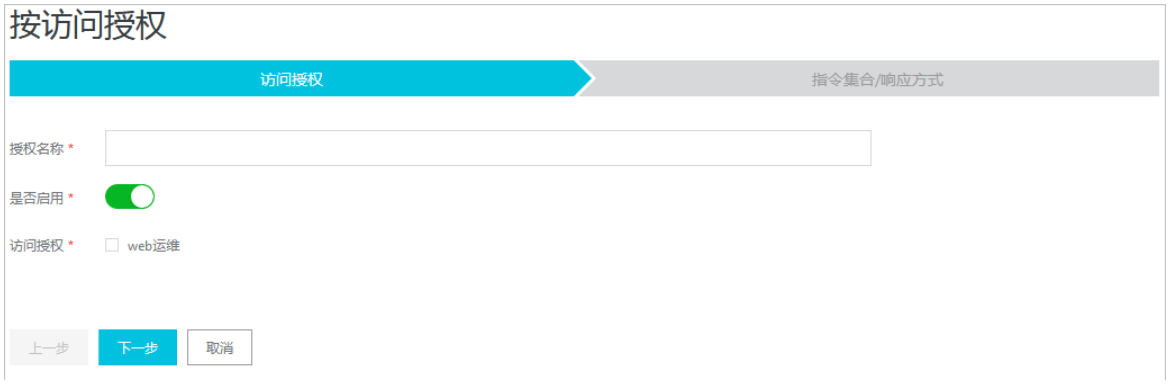
指令授权是指允许或拒绝选定的用户在目标主机上执行某些命令。按访问授权的方式，表示您直接使用访问授权中已设置的用户和目标主机。

前提条件

已创建访问授权策略，具体请参见配置访问授权。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏选择**运维管理**，在**资产管理**页面的**授权管理**页签，单击**按访问授权**。
4. 选择**访问授权**，设置授权名称和选择访问授权策略，单击**下一步**。



配置项	说明
授权名称	输入指令策略的名称。
是否启用	设置该指令授权策略是否启用。
访问授权	选择已设置的访问授权策略。 创建访问授权策略操作，具体请参见配置访问授权。

5. 在**指令集合/响应方式**中，设置指令授权的指令和响应方式，单击**保存**。



设置项	说明
配置指令集合	可配置允许或禁止使用以下指令（指令集）。
手工输入指令	可手工输入指令，多个指令请使用换行符分隔。
指令集合	在下拉栏中选择已设置好的指令集合。
响应方式	如果符合该指令规则，堡垒机的响应方式。 ○ **产生告警**：当触发该指令策略时堡垒机会生成告警事件。 ○ **阻断会话**：当触发该指令策略时堡垒机会将该会话连接中断。 ○ **忽略指令**：当触发该指令策略时堡垒机会将该指令忽略，不执行此命令并提示该指令未找到，会话可继续正常操作。 ○ **审批指令**：当触发该指令策略时会话会暂停等待管理员审批，管理员审批通过后指令会执行并可继续进行其他操作，如果管理员拒绝则指令不会执行但可以继续进行其他操作。
审批策略	可选，只有**响应方式**包含**审批指令**时需要设置。 从下拉栏中选择已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。

设置项	说明
告警信息	可选，只有**响应方式**包含**产生告警**时需要设置。 从下拉栏中选择已设置好的告警事件。如果没有可选择的告警事件，可以从下拉栏中单击**新增**，新增告警事件。新增告警事件的操作请参见创建事件告警。

10.9.2.5. 资源管理

10.9.2.5.1. 创建服务器集合

在服务器集合中，您可将运维主机或主机组配置成集合。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏选择**运维管理**，在**资源管理**页签单击**服务器集合**。
4. 单击**创建**。
5. 设置服务器集合的名称和范围，单击**保存**。



设置项	说明
名称	输入服务器集合的名称。
IP限制	是否启用IP限制功能，启用后集合只包括指定IP范围内的主机。 ○ **IP地址**：设置IP地址，单击+可添加多个IP。 ○ **IP区间**：设置IP起始和结束的范围，单击+可添加多个IP区间。

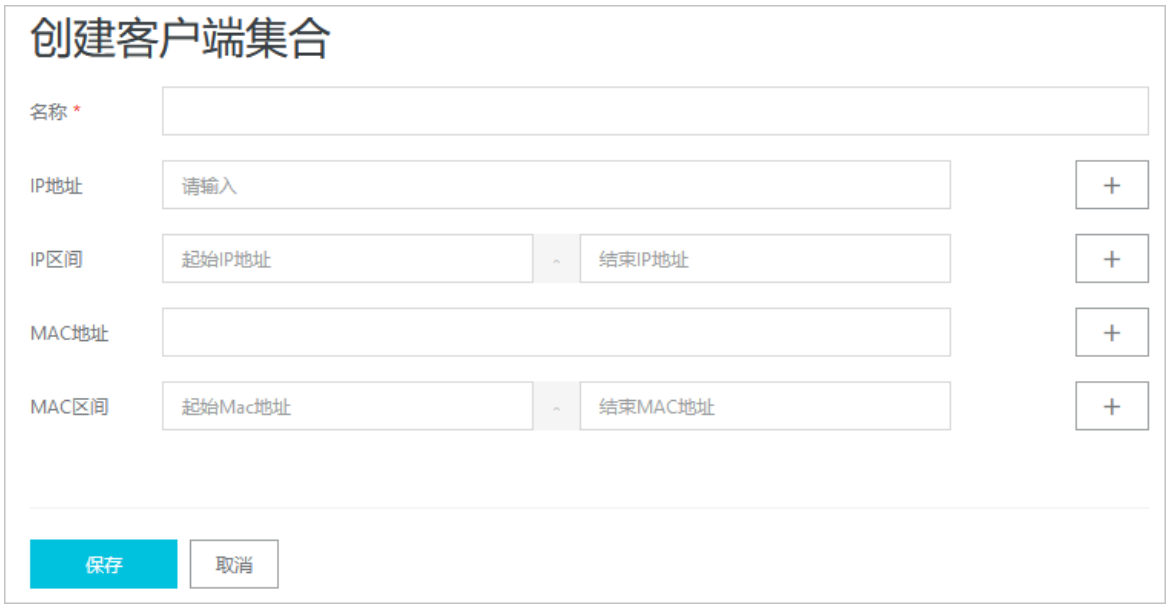
设置项	说明
主机	选择服务器集合中包含的主机或主机组。 ○ 选中**组授权**：表示选择该主机组下所有主机。 ○ 选中具体主机：表示选择已选中的主机。

10.9.2.5.2. 创建客户端集合

在客户端集合中，您可将IP/IP区间、MAC/MAC区间配置成集合。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏，选择**运维管理 > 资源管理**，单击**客户端集合**。
4. 单击**创建**。
5. 设置客户端集合的名称和范围，单击**保存**。



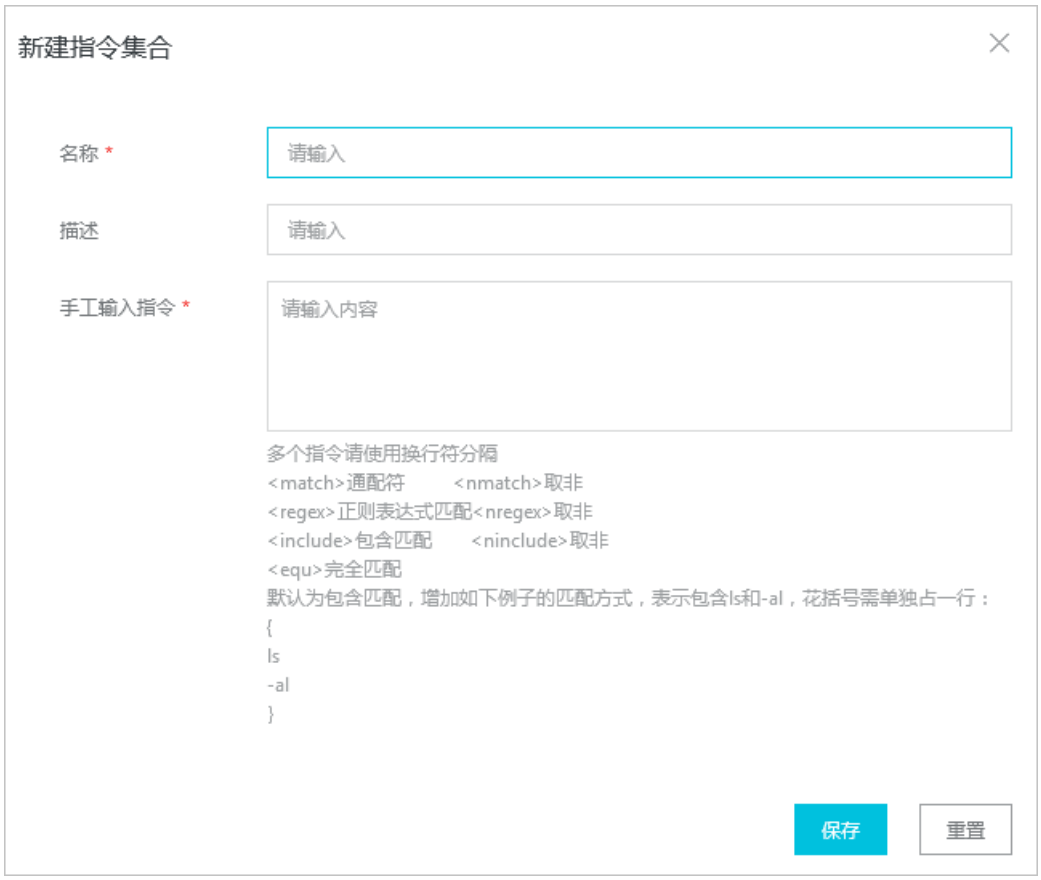
设置项	说明
名称	输入客户端集合的名称。
IP地址	设置IP地址，单击+图标可添加多个IP。
IP区间	设置IP起始和结束的范围，单击+图标可添加多个IP区间。
MAC地址	设置MAC地址，单击+图标可添加多个MAC。
MAC区间	设置MAC起始和结束的范围，单击+图标可添加多个MAC区间。

10.9.2.5.3. 创建指令集合

指令集合可将操作指令配置成集合。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在**运维管理**页面，单击**资源管理**。
4. 在**资源管理**页签下，单击**指令集合**。
5. 在**指令集合**页面，单击**创建**。
6. 设置指令集合，单击**保存**。



设置项	说明
名称	输入指令集合的名称。
描述	输入指令集合的详细描述信息，建议填写指令集合的用途等信息。
手工输入指令	可手工输入指令，多个指令请使用换行符分隔。

10.9.2.5.4. 创建审批策略

审批策略中可配置审批通知方式。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在**运维管理**页签下，单击**资源管理**页签。
4. 在**资源管理**页签下，单击**审批策略**。
5. 单击**创建**。
6. 设置审批策略，单击**保存**。



设置项	说明
名称	输入审批策略的名称。
方式	选择审批通知方式，支持**消息**、**短信**和**邮件**。
短信默认	可选，只有**方式**为**短信**时需要设置。 在下拉栏中选择默认短信网关，短信网关设置请参见设置短信网关。
短信备用	可选，只有**方式**为**短信**时需要设置。 在下拉栏中选择备用短信网关，短信网关设置请参见设置短信网关。
邮件默认	可选，只有**方式**为**邮件**时需要设置。 在下拉栏中选择默认邮件服务器，邮件服务器设置请参见设置邮件。

设置项	说明
邮件备用	可选，只有**方式**为**邮件**时需要设置。 在下拉栏中选择备用邮件服务器，邮件服务器设置请参见设置邮件。

10.9.2.5.5. 创建事件告警

事件告警中可配置违规操作、高危操作和异常登录事件的告警通知方式。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 在左侧导航栏，选择**运维管理**，在**资源管理**页签单击**事件告警**。
4. 单击**创建**。
5. 设置事件告警策略，单击**保存**。



设置项	说明
名称	输入事件告警的名称。
描述	输入事件告警的描述信息。
等级	设置事件的严重等级，支持**无**、**低**、**中**和**高**。
类型	选择事件的类型，支持**无**、**违规操作**、**高危操作**和**登录异常**。

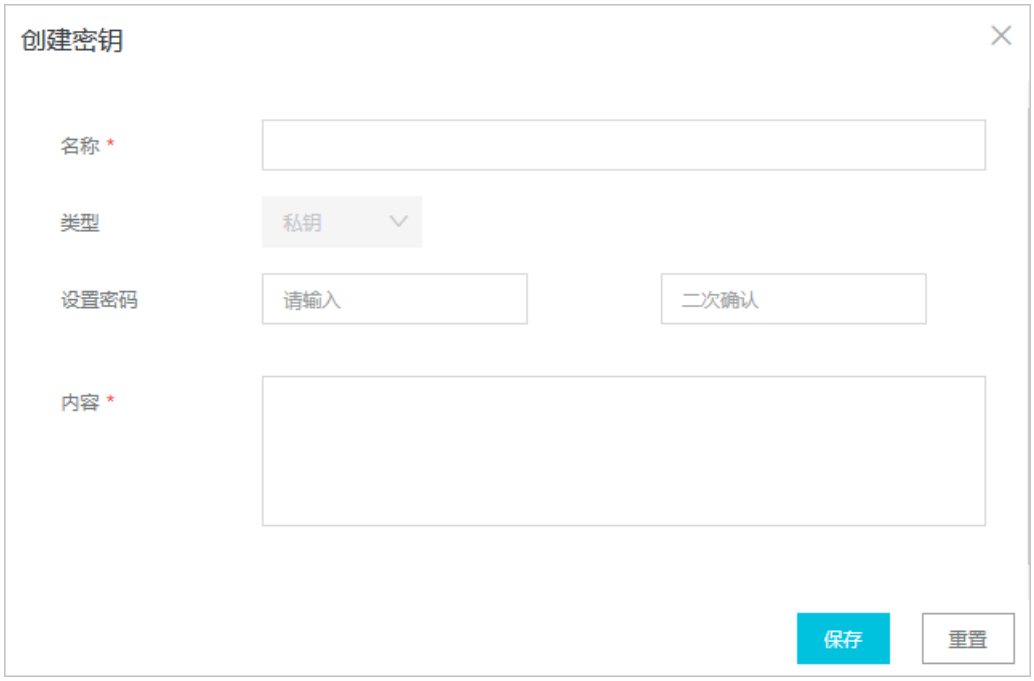
设置项	说明
方式	选择告警通知方式，支持**无**、**邮件**和**短信**。
默认	可选，只有**方式**为**邮件**或**短信**时需要设置。 在下拉栏中选择默认邮件或短信网关。 ○ 邮件服务器设置请参见设置邮件。 ○ 短信网关设置请参见设置短信网关。
备用	可选，只有**方式**为**邮件**或**短信**时需要设置。 在下拉栏中选择备用邮件或短信网关。 ○ 邮件服务器设置请参见设置邮件。 ○ 短信网关设置请参见设置短信网关。 ○

10.9.2.5.6. 创建密钥

在密钥管理中，您可以添加SSH认证私钥，用于堡垒机通过密钥方式登录被运维主机。已创建私钥可通过密码录入下发给指定主机账号。

操作步骤

1.
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 单击**运维管理**。
4. 在**运维管理**页面，单击**资源管理**页签。
5. 单击**密钥管理**。
6. 单击**创建**。
7. 设置密钥名称和内容，单击**保存**。



设置项	说明
名称	输入密钥的名称。
类型	固定为**私钥**。
设置密码	可选，为私钥设置密码并确认密码。 **说明** 如果需要密钥方式免密登录，则此处密码设置为空。
内容	输入私钥内容。

10.9.2.6. 密码管理

10.9.2.6.1. 密码录入

通过密码录入，您可以为指定的主机账号统一设置密码/密钥。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**密码管理**，单击**密码录入**。
4. 选择主机账号并设置主机账号对应的**密码**和**密钥**，单击**保存**。



设置项	说明
主机	选择要录入的密码或密钥对应的主机账号。
密码	可选，只有选中后才会生效。 输入并确认主机账号对应的密码。选中**空密码**表示设置空密码。
密钥	可选，只有选中后才会生效。 从已创建的密钥中选择主机账号对应的密钥。如果没有创建过密钥，您可以选择**新增**并创建密钥。创建密钥的操作请参见创建密钥。

5. （可选）如果选择了多个主机账号，根据页面提示确认统一修改密码。



执行结果

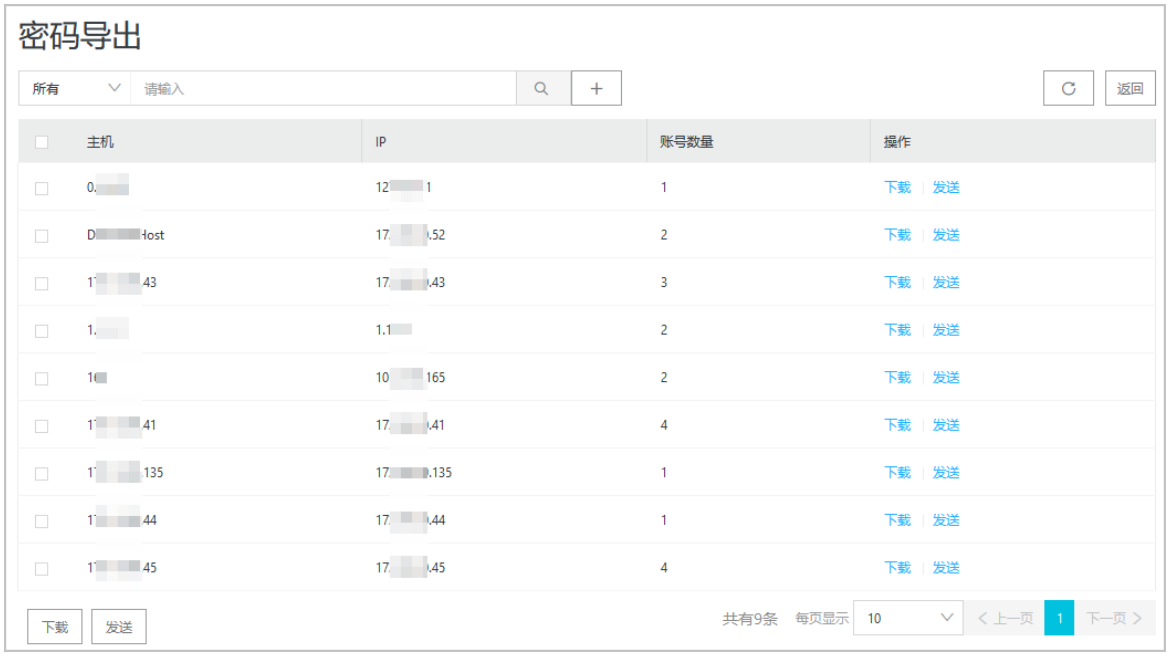
页面提示保存成功，表示成功录入密码。

10.9.2.6.2. 密码导出

通过密码导出，您可以将指定主机账号的密码下载到本地或发送给管理员。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**密码管理**，单击**密码导出**。
4. 选中标主机并选择**下载**或**发送**主机账号的密码。



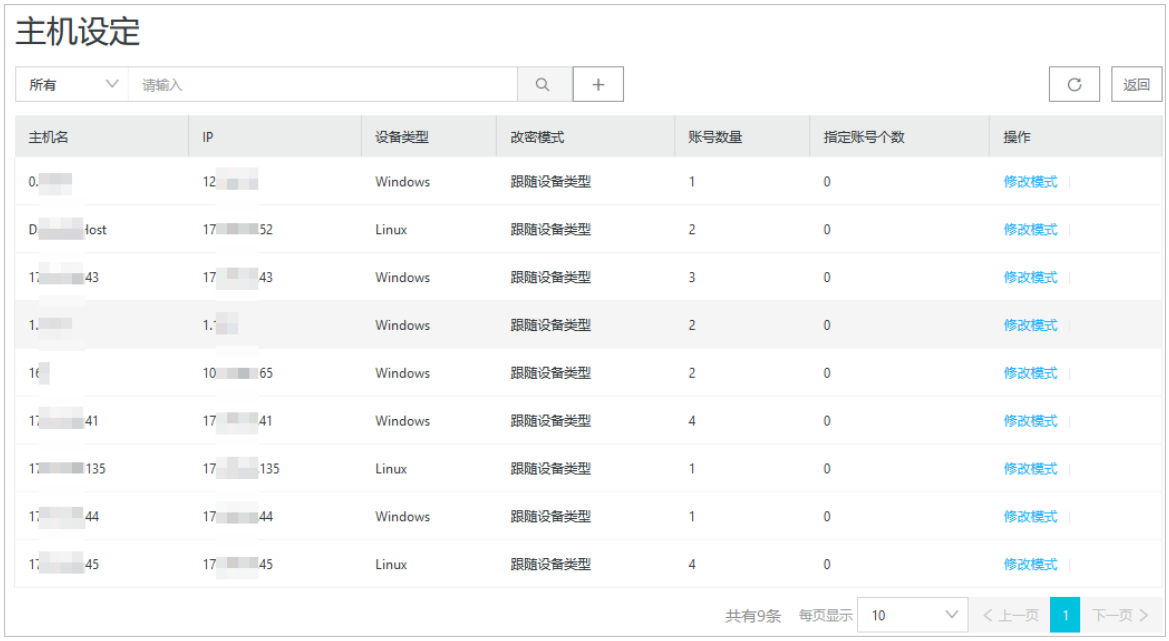
- **下载**：下载主机账号密码文件。下载的密码文件需要通过密码查看器查看。
- **发送**：将主机账号的密码文件通过设定的发送方式发送给管理员。

10.9.2.6.3. 主机设定

通过主机设定，您可以设定运维主机和账号的改密模式。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**密码管理**，单击**主机设定**。
4. 定位到要操作的主机，单击其操作列下的**修改模式**。



5. 选择**主机**页签，设置主机改密模式，并单击**保存**。



设置项	说明
改密方式	默认为**跟随设备类型**，支持选择**自定义**。
改密配置	默认为主机对应设备类型的默认改密配置，例如主机设备类型为Windows，则改密配置默认为**Windows改密配置**。支持选择**新增**，并自定义改密配置的名称。

设置项	说明
改密脚本	使用默认改密配置时，改密脚本为**默认**且不可修改。 使用自定义改密配置时，支持使用**默认**改密脚本或选择**自定义**，自定义改密脚本。
脚本	仅在**改密脚本**为**自定义**时需要配置。 输入自定义改密脚本。
连接方式	仅在**改密脚本**为**默认**时需要配置。 选择改密配置的连接方式。

6. 选择**账号**页签，单击账号操作列下的**修改模式**，自定义账号改密模式。



账号的**改密方式**默认为**跟随主机**。您可以参照自定义主机改密模式的操作，自定义账号改密模式。



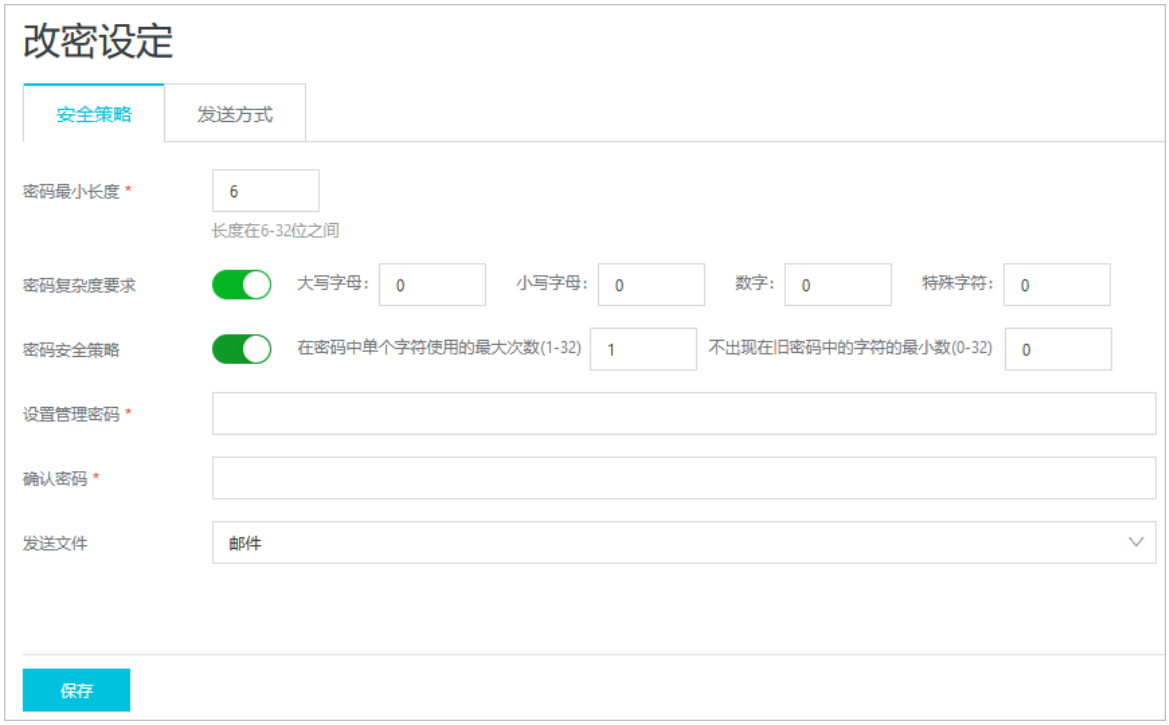
10.9.2.6.4. 改密设定

通过改密设定，您可以配置自动改密时密码的生成规则和发送方式。

操作步骤

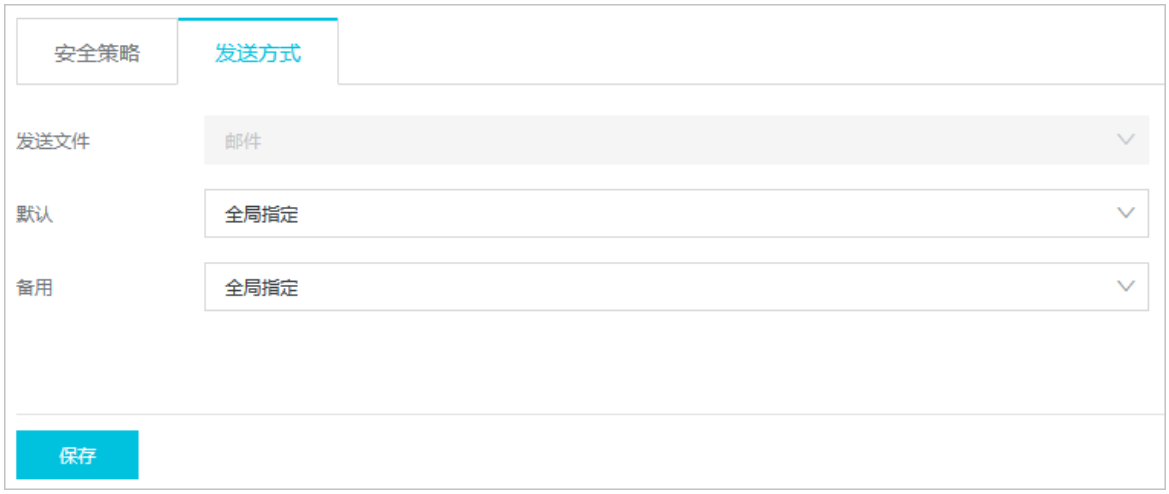
1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。

3. 选择**密码管理**，单击**改密设定**。
4. 选择**安全策略**页签，配置自动改密时密码的生成规则，单击**保存**。



设置项	说明
密码最小长度	设置改密时随机生成密码的最小长度。
密码复杂度要求	开启后，可以设置改密时随机生成密码必须包含的字符类型及位数。支持的字符类型包括**大写字母**、**小写字母**、**数字**、**特殊字符**。
密码安全策略	开启后，可以设置改密时随机生成密码最多允许出现的重复字符的个数。具体支持以下配置项： ○ **在密码中单个字符使用的最大次数** ○ **不出现在旧密码中的字符的最小数**
设置管理密码	为密码文件设置查看密码。
确认密码	确认密码文件的查看密码。
发送文件	设置密码文件的发送方式，可选值：**邮件**、**FTP**。

5. 选择**发送方式**页签，配置密码文件的发送方式，单击**保存**。



支持邮件和FTP两种方式，**发送文件**固定为步骤4中设置的**发送文件**方式。

- **发送文件**为**邮件**时，可以选择已设置的邮件发送方式，默认为**全局指定**。创建邮件发送方式的操作请参见设置邮件。
- **发送文件**为**FTP**时，可以在选择已设置的FTP发送方式，默认为**全局指定**。创建FTP发送方式的操作请参见设置FTP。

10.9.2.6.5. 自动改密

通过自动改密，您可以创建并管理自动改密计划。

前提条件

已完成改密设定。更多信息，请参见改密设定。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**密码管理**，单击**自动改密**。
4. 在**改密对象配置**中，设置改密计划的名称和对象，单击**下一步**。



设置项	说明
名称	填写改密计划的名称。特殊字符仅支持下划线（_）、短划线（-）和小数点（.）。
发送预备改密文件	是否发送预备改密文件。开启后，则自动改密计划执行前会发送预改密密码，管理员收到文件后，需要在堡垒机消息中确认，自动改密计划才会继续执行。
改密对象	通过**对象指定** 或**范围指定**方式指定要修改密码的主机账号。 ○ **对象指定**：直选中选具体的主机账号。 ■ 选中**组托管**：表示选中该组主机下的所有账号。 ■ 选中**主机托管**：表示选中该主机下的所有账号。 ○ **范围指定**：选择一定范围内主机下的账号。 ■ **服务器范围**：选择已定义的服务器合集，单击**+**可以选择多个服务器合集。 ■ 账号范围：选择访问服务器合集的账号范围。 ■ 选择**已定义**，则在**账号**中只能选择服务器合集中的主机关联的账号。 ■ 选择**自定义**，则在**账号**中可以选择堡垒机中创建的所有账号。 ■ **账号**：选择访问服务器合集中主机所使用的账号。 ■ **所有**：**账号范围**限定内的所有账号。 ■ **指定**：选择具体账号。 ■ **服务**：选择需要用到的主机服务。 ■ **所有**：**服务器范围**中所有的服务类型。 ■ **指定**：选择具体服务类型。

5. 在**改密策略配置**中，设置改密计划的开始时间和重复周期等信息，单击**保存**。



设置项	说明
策略名称	可选。从下拉栏中选择**新增**可将配置信息保存为模板，方便后续直接引用模板。添加新策略时需要设置策略名称。
开始时间	设置改密计划的开始执行时间。
重复周期	设置重复执行当前改密计划的周期，单位为**天**或**分钟**。
密码策略	设置自动改密计划的密码生成策略，可选项： ○ **随机生成不同密码** ○ **随机生成相同密码** ○ **人工指定相同密码**：使用该策略时，必须设置密码。
发送方式	选择密码发送方式，支持**邮件**与**FTP**方式。默认使用改密设定中指定的方式。

执行结果

成功创建自动改密计划后，页面跳转到**自动改密**管理页面。您可以在此查看改密计划的执行状态和结果，并根据需要停用或启用改密计划、修改改密计划、删除改密计划。



10.9.2.6.6. 手工改密

通过手工改密，您可以统一修改指定主机账号的密码。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**密码管理**，单击**手工改密**。
4. 选中要改密的**主机**账号，设置并确认**新密码**，单击**执行**。



执行结果

手工改密任务直接执行并返回改密结果。

10.9.2.7. 审计管理

10.9.2.7.1. 查看实时监控信息

管理人员通过查看堡垒机的实时监控信息，了解整体运维情况。

操作步骤

1. 登录云盾安全中心。

2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 单击**实时监控**，查看堡垒机的实时运维情况。



监控项	说明
系统概要	查看堡垒机的运行状态，包括以下信息： ○ 运维用户、运维主机、访问策略、指令策略的统计数量。 ○ 操作、会话、异常操作和异常会话的当日和当月统计数量。
时间趋势	查看全部（或异常）的操作和会话的变化趋势。
运维用户	查看运维用户产生的运维操作或会话的统计数量。
告警	查看堡垒机告警列表。
协议	查看当天（当月）协议的操作或会话统计数量。
服务器	查看运维主机产生的运维操作或会话的统计数量。
最新会话	查看最新产生的会话连接信息。

10.9.2.8. 消息中心

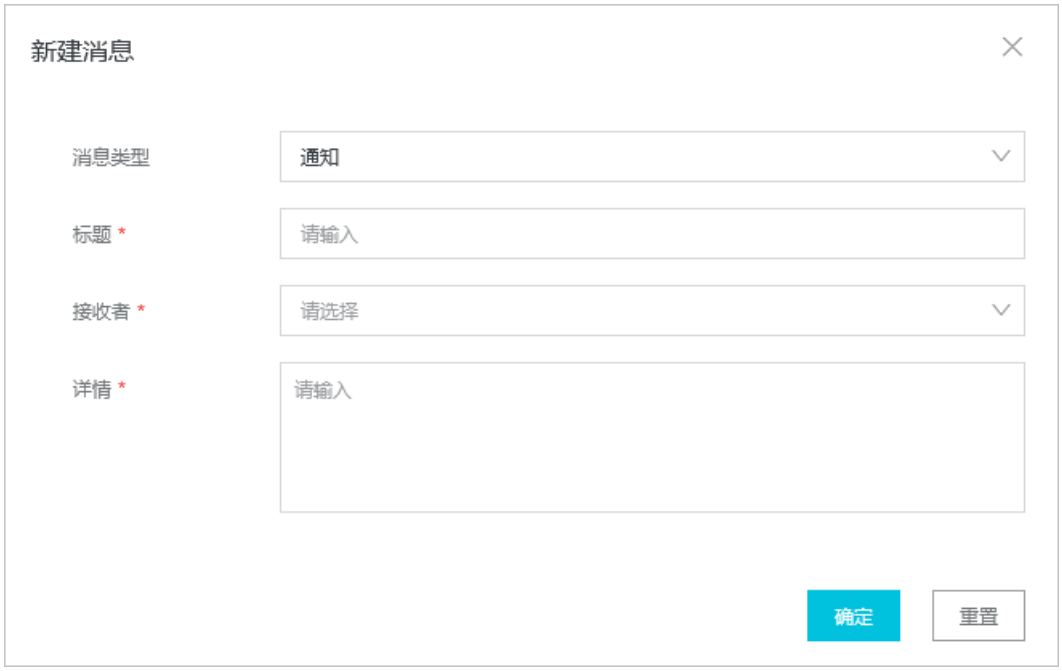
10.9.2.8.1. 发送消息

本文介绍如何在堡垒机中给其他用户发送消息。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。

3. 选择**消息中心**。
4. 单击**发送**页签。
5. 单击**新建消息**。
6. 选择消息类型并填写消息，单击**确定**，发送消息。



消息项	说明
消息类型	在下拉框中选择消息类型，仅支持**通知**。
标题	输入消息的标题。
接收者	在下拉框中选择消息接收人，可选择多个人员群发消息。
详情	输入消息的详细信息。

10.9.2.8.2. 查看消息

在消息中心查看接收到的消息。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏中，选择**运维审计 > 堡垒机**，单击堡垒机实例的**详情**。
3. 选择**消息中心 > 接收**。
4. 在消息列表中查看信息。

10.9.3. 运维员操作指南

10.9.3.1. 登录堡垒机运维环境

本文介绍运维人员如何登录堡垒机的运维环境。

前提条件

管理员已经为运维人员创建用户并设置运维访问授权，具体操作请参见创建用户和配置访问授权。

管理员获取堡垒机的运维地址

此步骤由管理员操作，登录云盾安全中心获取堡垒机的运维地址，具体操作如下：

1. 登录云盾安全中心。
2. 在控制台上方单击**安全**，选择到**运维审计 > 租户堡垒机**，在堡垒机实例列表查看目标堡垒机的运维地址。



> **说明** **私网IP地址**：运维人员的客户端需要能够访问堡垒机所在的VPC，才能通过**私网IP地址**登录堡垒机。

3. 管理员将堡垒机运维地址发送给运维人员。

运维人员登录堡垒机运维环境

此步骤由运维人员操作，登录堡垒机运维环境，具体操作如下：

1. 运维人员从管理员处获取堡垒机运维地址。
2. 在浏览器地址栏中，输入堡垒机运维地址，按回车键。

   堡垒机的登录格式如下：

   ```
   https://<堡垒机运维地址>
   ```

3. 输入正确的用户名和密码，单击**登录**。

> **说明** 运维人员的用户名和密码请从管理员处获取。



10.9.3.2. 安装运维客户端

在使用堡垒机运维前，需要安全运维客户端（Bhost Client）。本文介绍如何安装Bhost Client。

操作步骤

1. 登录堡垒机运维环境。
2. 在左侧导航栏中选择**访问工具**，单击**相关下载**。
3. 单击**Bhost Client**，将客户端文件（*BHost Client.exe*）下载到本地。
4. 在本地主机中，双击*BHost Client.exe*，根据提示默认安装完运维客户端。

10.9.3.3. 通过Web方式运维

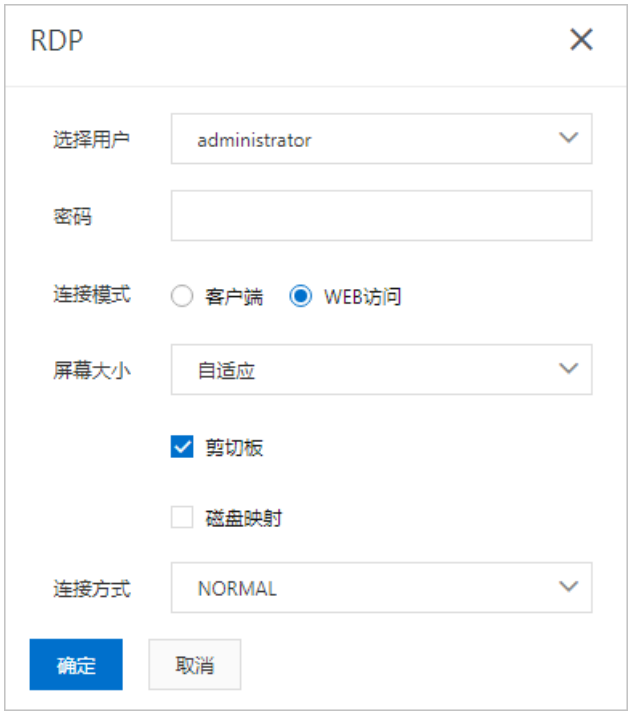
本文介绍运维人员如何在堡垒机中通过Web方式运维主机。

背景信息

通过Web方式运维支持RDP、SSH、SFTP等常用协议，本文以RDP为例。

操作步骤

1. 登录堡垒机运维环境。
2. 在左侧导航栏中单击**主机分组**。
3. 在**全部分组**中，定位到目标主机所在的分组。
4. 在主机列表中，单击**运维协议**（例如**RDP**）。
5. 在登录对话框中，设置登录信息，单击**确定**。



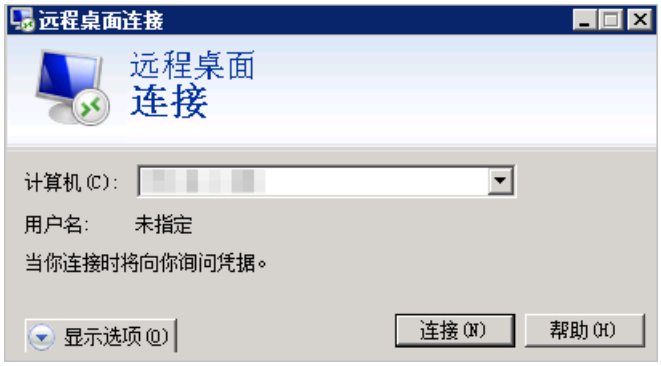
- 在**选择用户**选择登录主机的账号。
- 在**密码**中输入主机账号的登录密码。
- 在**连接模式**中选择运维模式，此步骤选择**WEB访问**。

10.9.3.4. 通过客户端方式运维

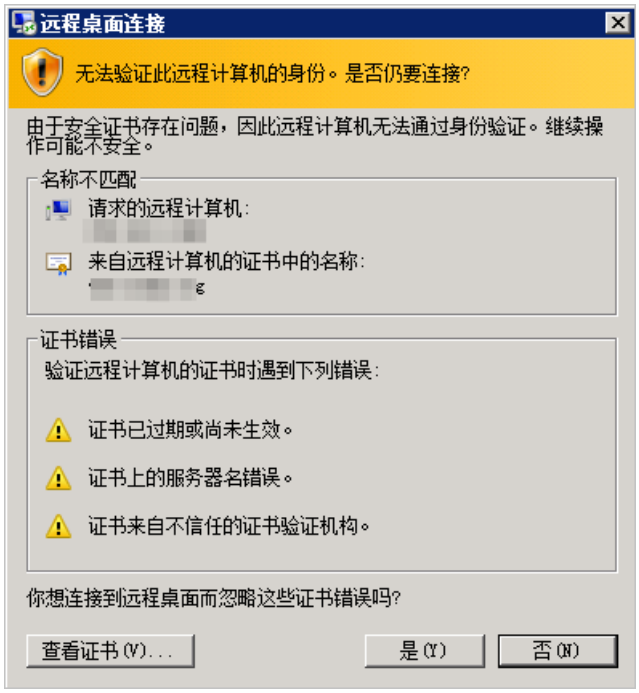
本文介绍通过客户端方式运维主机，包括RDP协议运维和SSH协议运维。

RDP协议运维

1. 运维人员在本地主机打开远程桌面连接工具（Mstsc）。
2. 输入堡垒机运维地址，单击**连接**。



3. 在**远程桌面连接**提示框中，单击**是**。



4. 在堡垒机**登录**窗口，输入运维人员的账号和密码，单击**确定**。

> **说明** 运维人员的账号和密码请从管理员处获取。

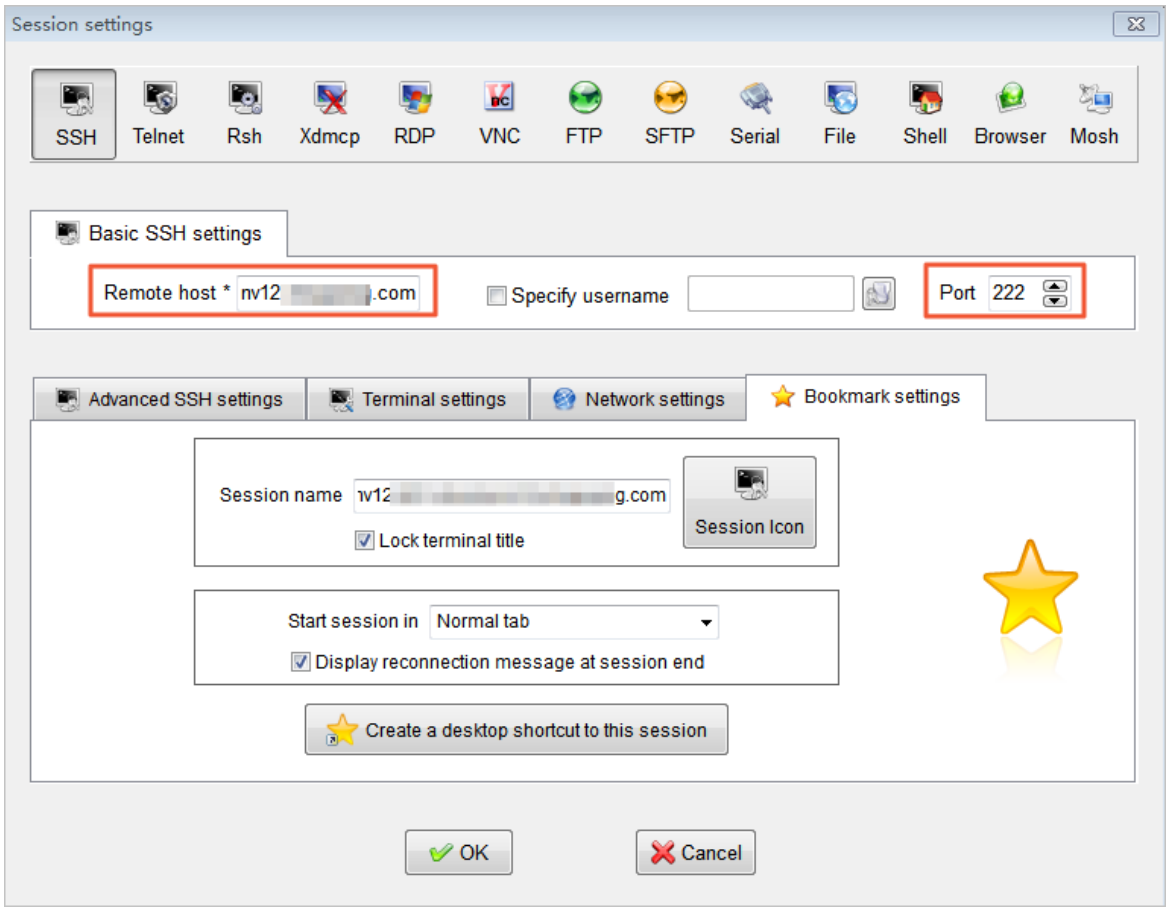


5. 选择运维主机的**设备**、**主机服务**和**账号**，单击**确定**登录主机。



SSH协议运维

1. 运维人员在本地主机打开SSH连接工具（例如MobaXterm）。
2. 输入堡垒机的运维地址和端口号（222），单击**OK**。



3. 输入运维人员的堡垒机账号，按回车键（Enter），再输入密码，按回车键（Enter）。



4. 通过上、下方向键依次选择主机组、主机、协议（SSH）和主机账户，按回车键（Enter）。



5. 输入账户密码，按回车键（Enter），登录目标主机。

10.10. 平台侧堡垒机

10.10.1. 概述

平台侧堡垒机为云服务器的运维提供完整的权限控制和审计回放服务。

平台侧堡垒机基于账号（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。

10.10.2. 工具下载

在进行服务端配置前，需要先下载安装平台侧堡垒机的插件。

操作步骤

1. 在浏览器地址栏中，输入平台侧堡垒机运维管理系统的访问地址，按回车键。
2. 使用admin账号登录运维管理系统页面。
3. 单击**访问工具 > 相关下载**。
4. 在**相关下载**页面单击需要安装的插件。
   - **BHost Replay**：用于播放离线的审计录像。

     > **说明** 管理员角色建议安装这个版本的客户端，如果您之前已经安装了 BHost Client 客户端， 需要先卸载再安装BHost Replay。

   - **密码查看器**：查看下载的密码文件时需要安装。
   - **BHost Client**：运维用户必须安装，运维及配置的插件。

     > **说明** 建议运维用户将软件安装在D盘，如果没有D盘的安装在*C:\Program Files*路径下。

- BHostAgent：做Windows自动改密时使用，安装在Windows主机上。

10.10.3. 管理员操作指南

10.10.3.1. 实时监控

实时监控对堡垒机整体情况进行概要性展示，以便安全管理员快速了解和掌握平台侧堡垒机的信息。

在云盾安全中心的**运维审计 > 平台侧堡垒机 > 实时监控**中，可以查看**系统概要**、**告警信息**、**时间趋势**、**会话协议**、**运维用户**、**最新会话**。



- **系统概要**：展示堡垒机运行状态信息。可查看当前系统时间、运维用户数量、运维主机数量、访问策略和指令策略数量。

  单击**日志**进入**系统日志**页面，可查看系统运行、系统配置、用户登录、用户配置、用户检索等日志。

- **告警**：展示及处理系统告警日志。

  单击**更多**可查看告警详情。

- **时间趋势**：以时间为基线，展示每小时/天产生运维操作、会话量趋势。
  - 全部、异常：单击可切换显示所有运维操作、会话或异常操作、会话。
  - 操作、会话：单击可切换显示运维操作、会话量。
  - 图表展示区：可单击某个时间点，查看该时间内运维操作、会话的统计与详细数据。

- **运维用户**：以运维用户为基线，展示运维用户产生的运维操作、会话量统计。
  - 全部、异常：单击可切换显示运维用户产生的运维操作、会话或异常操作、会话。
  - 操作、会话：单击可切换显示运维用户产生的运维操作、会话量。
  - 图表展示区：可单击运维用户，查看该用户运维操作、会话的统计与详细数据。

- **服务器**：以服务器为基线，展示运维主机产生的运维操作、会话量统计。
  - 全部、异常：单击可切换显示运维主机产生的运维操作、会话或异常操作、会话。
  - 操作、会话：单击可切换显示显示运维主机产生的运维操作、会话量。
  - 图表展示区：可单击运维主机IP地址，查看该主机运维操作、会话的统计与详细数据。

- **协议**：以运维协议为基线，基于协议的角度来统计、展示运维协议。
- **最新会话**：展示当前正在连接的或者当天已经连接过的会话列表。

检索出来的记录可以进行实时监控、在线回放、关联分析、下载回放文件。在线回放前需要下载和安装BHost Replay工具，请参见工具下载。

10.10.3.2. 数据检索

本文介绍如何对历史会话、操作及系统日志的内容进行检索。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云原生堡垒机**，单击平台侧堡垒机实例的**详情**。
3. 在左侧导航栏，选择**数据检索**。
4. 在**检索**页签，设置日志类型、索引条件等检索条件。



   - 单击**添加**，可以添加多个检索条件。
   - 您可单击**保存**将常用检索条件保存为模板，需要使用时在**导入模板**选择该模板。
5. 单击**检索**，对满足检索条件的历史会话、操作及系统日志的内容进行检索。

   可对检索出来的记录进行详情查看、指令查看、在线回放、关联分析、下载回放文件。

   > **说明** 在线回放前需要下载和安装BHost Replay工具，请参见工具下载。

   在**历史任务**页签，可以查看检索历史、查询历史检索结果、使用历史检索条件。

10.10.3.3. 运维报表

本文介绍如何根据已配置的报表手动、周期生成报表。

操作步骤

1.
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云原生堡垒机**，单击平台侧堡垒机实例的**详情**。
3. 在左侧导航栏，选择**运维报表**。
4. 在**模板**中选择报表模板。
5. 在**报表条件**页签，检查并设置报告模板中统计报告的信息。
6. 单击**报表详情**页签，查看报告的基本信息、报表条件、基础报表。

如需定期生成计划报表，开启计划任务，选中日报、周报、月报选项，可指定报表以邮件方式发送。

7. 在**报表条件**页签，单击**执行**。

   生成指定的报表后，单击**任务列表**可以查看统计报告详情。

10.10.3.4. 用户管理

10.10.3.4.1. 配置全局安全策略

配置堡垒机的全局安全策略。安全策略保障用户账号的安全性。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云原生堡垒机**，单击平台侧堡垒机实例的**详情**。
3. 在左侧导航栏，选择**运维管理**，在**运维管理**页签单击**全局策略**。
4. 在**安全策略**页签，设置全局安全策略，单击**保存**。



设置项	说明
密码最小长度	设置堡垒机用户登录密码位数，最小为6位，最大为32位，缺省为8位。
密码使用期限	设置密码有效期，用户在密码到期前必须修改密码。 系统可设置密码过期提示天数，在密码过期前提示用户修改密码，0表示不提示。
密码复杂程度要求	设置密码必须包含哪类字符。
密码安全策略	设置密码不允许重复使用的次数。

设置项	说明
账户锁定策略	设置账号锁定策略及账号锁定后的自动解锁时间。
登录验证	启用登录验证码后，用户登录时需要输入图片验证码。

10.10.3.4.2. 创建用户认证模式

用户登录堡垒机时需要登录认证，用于提高堡垒机的安全。该章节介绍如何配置认证模式和新增认证模块。

操作步骤

1.
2.
3. 在左侧导航栏，选择**运维管理**，在**运维管理**页签单击**认证模块**。
4. 在**认证方式**页面，单击**创建**。



设置项	说明
名称	输入认证方式的名称。
默认	启用后，该认证方式将作为创建用户时的默认认证方式。
验证方式	选择验证方式。 ○ **全部通过**：表示需要符合所有认证模块才能认证通过。 ○ **任一通过**：表示只需要符合一项认证模块，即可认证通过。
模块配置	在下拉栏中选择认证模块。 通过单击**+**，可以设置多个认证模块。

5. 单击**保存**。

10.10.3.4.3. 创建用户组及用户

该章节介绍如何创建、管理用户组及用户。

前提条件

已在**运维管理 > 认证模块**中创建认证方式，创建用户时也可直接新增认证方式。

创建用户组

1.
2.
3. 在左侧导航栏，选择**运维管理**，在**运维管理**页签的**查看与管理**区域单击**用户管理**。
4. 在**用户管理**页面左上角单击**创建用户组**，设置用户组名称、描述、访问授权。
5. 单击**保存**。

   在用户组列表的操作列可对创建的用户组进行修改、剪切、复制、删除操作。

创建用户

1.
2.
3. 在左侧导航栏，选择**运维管理**，在**运维管理**页签单击**系统用户**。
4. 在**新建用户**页面，输入用户信息。



参数	说明
启用	是否启用该用户，开启后该用户才可以使用。
账号	添加的用户名。
姓名	显示的用户名称。
描述	用户的描述。
认证方式	可选择默认或自定义认证方式。
访问授权	选择用户授权策略，可以自定义。
密码	可选择设置密码或使用初始密码。 如使用随机密码，可单击**随机密码**自动生成。
工号	用户的工号。

参数	说明
部门	用户所属的部门。
手机	用户的手机号。
Email	用户的邮箱信息。若管理员邮件接收改密文件或报表时，必须配置。

5. 单击**扩展选项**页签，在**扩展选项**页面设置第三方认证账号、唯一登录开关、失效时间开关。

   如果开启了**唯一登录**，当前用户只能同时在1 台终端上运维。

   如果该用户是临时用户，可设定账号失败时间。
6. 单击**用户组**页签，在**用户组**页面选中用户所属用户组。
7. 单击**保存**。

   在用户列表的操作列可对创建的用户进行修改、剪切、复制、交接、删除、移除操作。
   - **修改**：修改用户信息。
   - **剪切**：可从用户组A中选中一个用户，剪切到用户组B中去粘贴，从而实现将属于用户组A的用户移动到用户组B中去。
   - **复制**：可从用户组A中选中一个用户，在用户组B中粘贴，从而实现用户A同时属于用户组A和用户组B。
   - **删除**：将选中的用户删除，用户组列表中将不存在该用户。
   - **交接**：若某用户A临时请假，可在请假前将账号权限交接给用户B。
   - **移除**：将选中的用户从当前用户组中移除，其它用户组若还有该用户则不会被移除。

10.10.3.5. 主机管理

10.10.3.5.1. 创建主机账号

本文介绍如何在堡垒机中创建运维主机的账号。

背景信息

堡垒机已经存在部分默认的主机账号，部分默认账号的信息说明如下：

- *****：任意账号，允许用户在登录时自行填写。
- **-**：空账号，有密码但账号名为空，一般交换机中会出现。
- **#**：单点登录账号，与堡垒机登录的运维账号相同。

如果默认账号不能满足您的需求，您可以参照本文创建新的主机账号。

操作步骤

1.
2.
3. 在左侧导航栏，单击**运维管理**，在**运维管理**页签单击**主机账号**。
4. 在**账号**页签，单击**创建**。
5. 输入账号信息，单击**保存**。



设置项	说明
账号	输入账号名称。
AD域	可选项，选择账号的AD域服务器。

如果您需要同时添加多个账号，输入**账号**和选择**AD域**后，单击**+**图标，重新添加新的账号信息。

10.10.3.5.2. 创建主机的访问协议

本文介绍如何为堡垒机添加新的访问协议。

操作步骤

1.
2.
3. 在左侧导航栏，单击**运维管理**，在**运维管理**页签单击**访问协议**。
4. 在**协议**页面，单击**创建**。
5. 设置设备类型，单击**保存**。



配置项	说明
请选择	选择堡垒机支持的设备类型。
名称	输入设备名称。
账号切换命令	设备切换登录账号时使用的命令。
密码切换提示	设备切换登录账号时的密码提示符。
描述	输入设备的详细注释。
隐藏	是否隐藏该设备类型，隐藏后在创建主机过程中配置主机类型时将不能选择该设备类型。
配置服务	单击+添加主机的服务协议类型。

10.10.3.5.3. 创建主机组及主机

该章节介绍如何创建并管理主机组及主机。

创建用户组

1.
2.
3. 在左侧导航栏，单击**运维管理**，在**运维管理**页签的**查看与管理**区域单击**主机管理**。
4. 在**主机管理**页面左上角单击**创建主机组**，设置主机组名称、描述。
5. 单击**保存**。

   在用主机组列表的操作列可对创建的主机组进行编辑、剪切、复制、删除操作。

创建主机

1.
2.
3. 在**运维管理**页签，单击**主机**。
4. 在**创建主机**页面，输入主机基本信息、添加服务类型、添加主机账号、选中主机组。



设置项	说明
主机IP	输入主机的IP地址。 单击**Ping测试**，可以测试堡垒机和该主机之间的网络是否连通。
主机名	输入主机名称。 特殊字符仅支持英文、下划线、横杠、小数点 。
设备类型	在下拉框中选择设备的类型，可选择类型包括**Windows**、**Linux**、**Unix**等操作系统；**Cisco**、**Huawei**等各厂商硬件。
描述	输入该主机的备注内容，便于您后续查看和管理主机。
访问速度	选择访问速度，可选择**正常**、**较慢**或**很慢**。
唯一登录	启用后，该主机同一时间只允许一个用户连接。
启用	启用该主机。 ○ 在启用状态时，用户可以运维该主机。 ○ 在关闭状态时，用户不可以运维该主机，需要先启用该主机才能运维。
服务	单击**+**，设置需要运维的主机服务。 例如：主机为Linux，可以设置SSH、FTP、数据库等服务。
账号	单击**+**，设置需要运维的主机账号。 在堡垒机中创建主机账号的操作步骤请参见创建主机账号。
主机组	选中主机所属的主机组。

5. 单击**保存**。

   在主机列表的操作列可对创建的用户进行编辑、剪切、删除、复制、移除操作。

   - **编辑**：修改主机信息。
   - **剪切**：可从主机组A中选中一个主机，剪切到主机组B中去粘贴，从而实现将这台属于主机组A的主机移动到主机组B中。
   - **复制**：可从主机组A中选中一个主机，在组B中粘贴，从而实现主机A同时属于主机组A和主机组B。
   - **删除**：将选中的主机删除，主机组列表中将不存在该主机。
   - **移除**：将选中的主机从当前主机组中移除，其它主机组若还有该主机则不会被移除。

10.10.3.6. 运维管理

10.10.3.6.1. 配置全局运维策略

配置堡垒机的全局运维策略，全局运维策略的优先级高于访问授权策略中的权限配置。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**运维管理**，在**运维管理**页签单击**全局策略**。
4. 在**运维策略**页签，设置全局运维策略，单击**保存**。



设置项	说明
代填分隔符	仅支持and（&）、竖线（|）、at（@）。
超时设置	启用并设置阈值后，运维会话如果在该时间内无操作将断开连接。
运维访问通道	启用后所有运维访问会话都会通过运维访问通道进行连接，客户端与堡垒机运维访问通道端口必须保证通信正常，端口缺省为8088。

设置项	说明
文件传输记录	启用后可在**访问授权**中配置文件记录权限，并设置传输文件记录保存的最大存储空间。
隐藏主机IP	启用后运维用户界面无法查看主机IP，仅显示主机名称。
账号密码保存	选择运维访问时是否保存主机账号或密码，可选值：**提示**、**保存**、**不保存**。
应用发布访问控制	启用后应用发布客户端不允许访问除目标主机外的其他IP。
登录审批	启用后所有运维会话访问都需要通过管理员审批。 启用审批时可以应用已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。
访问备注	启用后所有运维会话访问都需要填写操作备注。
协同登录	启用后所有运维会话访问都需要邀请任意其他运维用户共同操作会话。
登录告警	选择登录告警策略，可选值：**不告警**、**登录告警**。 选择告警时可以应用已设置好的事件告警。如果没有可选择的事件告警，可以从下拉栏中单击**新增**，新增事件告警。新增事件告警的操作请参见创建事件告警。
指定应用发布	配置应用发布为**内置**或**外置**，以及外置应用发布服务器IP。

10.10.3.6.2. 配置访问授权

本文介绍如何配置用户与主机之间的访问关系及运维权限。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云原生堡垒机**，单击平台侧堡垒机实例的**详情**。
3. 在**平台堡垒机**页面左侧导航栏，单击**运维管理**。
4. 在**资产管理**页面，单击**授权管理**页签。
5. 在**授权管理**页签，单击**访问授权**。
6. 在**运维用户**中选择用户等信息，单击**下一步**。

设置项	说明
授权名称	输入访问授权策略的名称。
是否启用	设置该访问授权策略是否启用。
授权动作	设置访问授权的授权动作，可选**允许**或**拒绝**。 ○ **允许**：表示访问授权策略中的用户允许访问目标主机。 ○ **拒绝**：表示访问授权策略中的用户禁止访问目标主机。

设置项	说明
用户	选择访问授权策略生效的用户。 ○ 选中**组授权**，表示此访问授权策略对该组中所有用户都生效。 ○ 选中部分用户，表示此访问授权策略对已选择的用户生效。

7. 在**访问范围**中选择访问目标，单击**下一步**。

   访问目标可选择指定的具体服务、主机或主机组；也可以选择一定范围内的所有主机。

   ○ 选中**对象指定**页签，选择指定的具体服务、主机或主机组。



   ■ 选中**组授权**：表示此访问授权策略对该组中所有主机都生效。

   ■ 选中**主机授权**：表示此访问授权策略对该主机中所有服务都生效。

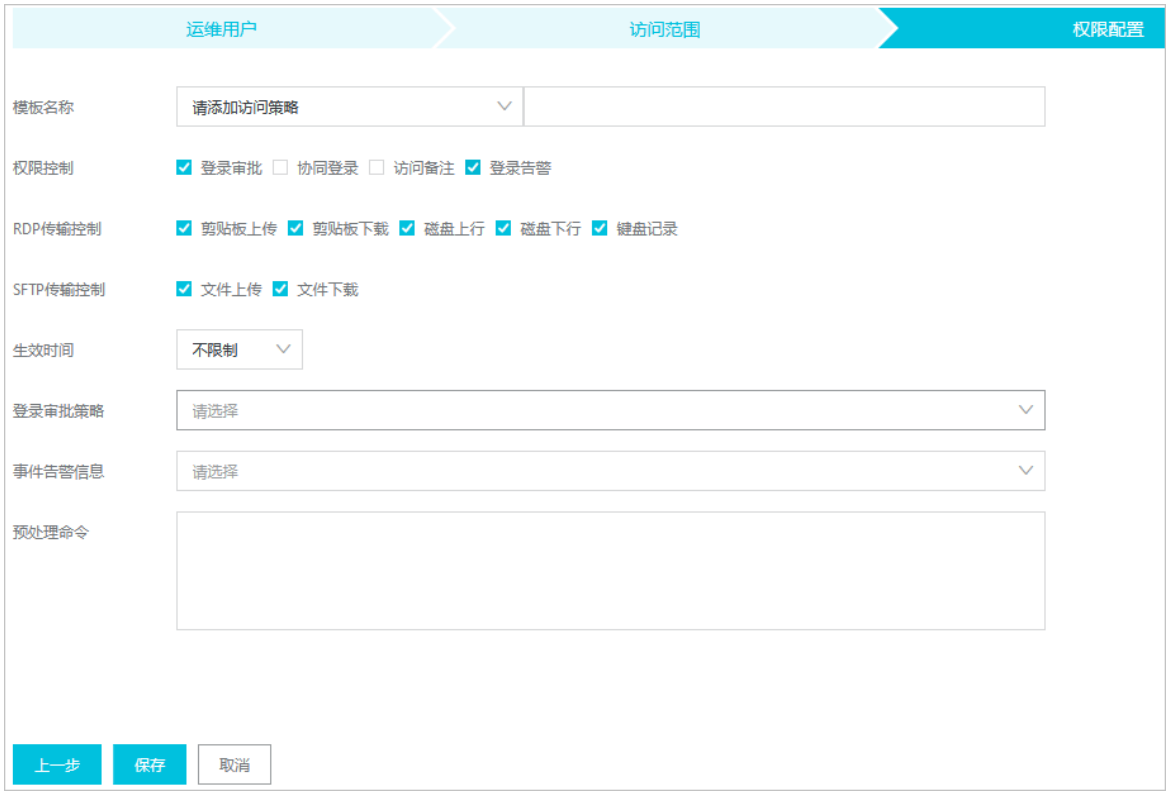
   ■ 选中具体服务：表示此访问授权策略对选中的服务生效。

   ○ 单击**范围指定**页签，选择一定范围内的所有主机。



设置项	说明
服务器范围	在下拉栏中选择服务器合集，单击 + 图标可以选择多个服务器合集。
账号范围	选择访问服务器合集的账号范围。 ■ 选择**已定义**，表示您在**账号**中只能选择服务器合集中的主机关联的账号。 ■ 选择**自定义**，表示您在**账号**中可以选择堡垒机中创建的所有账号。
账号	选择访问服务器合集中主机所使用的账号。 ■ **所有**：**账号范围**限定内的所有账号。 ■ **指定**：选择具体账号。
服务	单击 + 图标，设置需要运维的主机服务。 ■ **所有**：**服务器范围**中所有的服务类型。 ■ **指定**：选择服务类型。

8. 在**权限配置**中，设置访问授权的权限限制条件，单击**保存**。



设置项	说明
模板名称	在下拉栏中选择已配置模板，或在下拉栏中单击**新增**，输入模板名称，创建新的模板。
权限控制	选择用户登录主机时的权限控制策略。 ○ **登录审批**：用户每次访问主机时都需要经过管理员审批。 ○ **协同登录**：用户每次访问主机时需要邀请任意其他用户共同操作会话。 ○ **访问备注**：用户每次访问主机时需要填写访问主机的备注信息。 ○ **登录告警**：用户每次访问主机时触发登录告警。
RDP传输控制	使用RDP远程访问桌面服务时，是否允许**剪贴板上传**、**剪贴板下载**、**磁盘上行**、**磁盘下行**或**键盘记录**等操作。
SFTP传输控制	使用SFTP服务时，是否允许**文件上传**或**文件下载**操作。
FTP传输控制	使用FTP服务时，是否允许**文件上传**或**文件下载**操作。
生效时间	设置访问授权策略的有效时间范围。 ○ **不限制**：表示访问授权设置完成并启用后，该策略一直有效。 ○ **允许**：表示访问授权策略在允许的时间范围内，该策略有效。 ○ **例外**：表示访问授权策略在例外的时间范围内，该策略无效；在其他时间范围内，该策略生效。

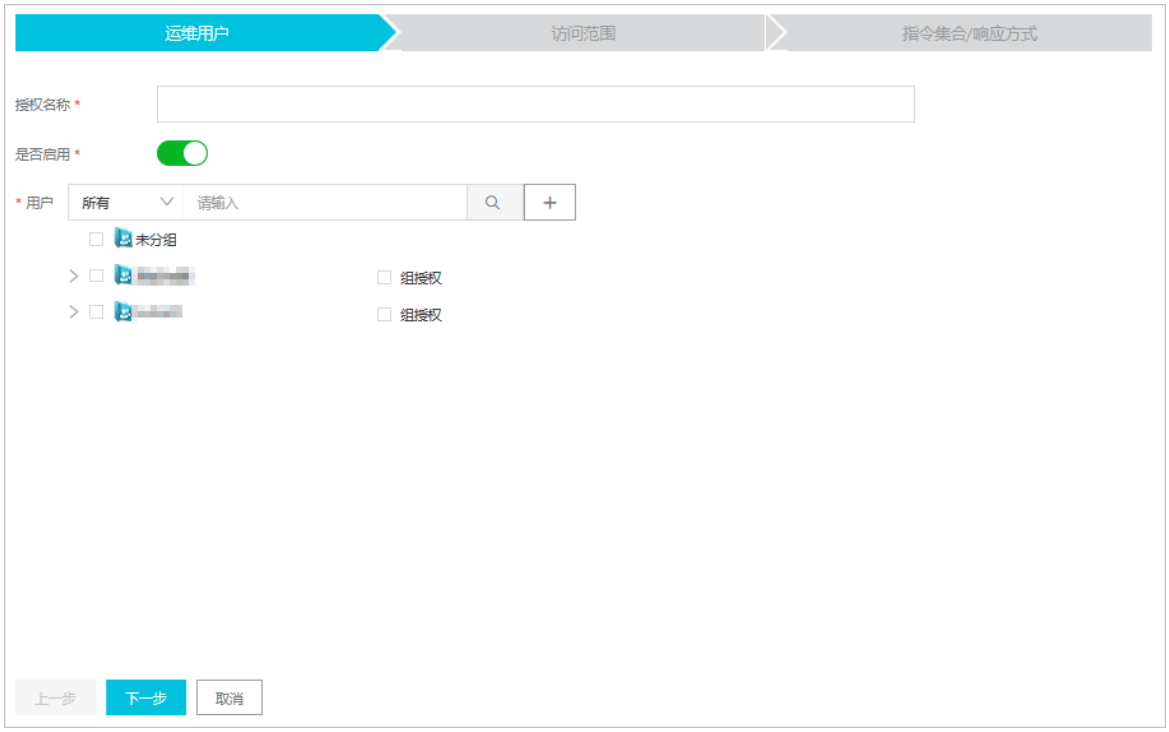
设置项	说明
登录审批策略	可选，只有**权限控制**包含**登录审批**时需要设置。 从下拉栏中选择已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。
事件告警信息	可选，只有**权限控制**包含**登录告警**时需要设置。 从下拉栏中选择已设置好的事件告警。如果没有可选择的事件告警，可以从下拉栏中单击**新增**，新增事件告警。新增事件告警的操作请参见创建事件告警。
预处理命令	运维用户每次连接主机后会自动执行该命令，仅限字符型会话（例如SSH），多个命令可用英文半角分号（;）分隔。

10.10.3.6.3. 配置指令授权（按对象授权）

指令授权是指允许或拒绝选定的用户在目标主机上执行某些命令。按对象授权的方式，表示您需要自己设定用户和目标主机。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**运维审计 > 平台侧堡垒机**。
3. 在左侧导航栏，单击**运维管理**，在**授权管理**页签单击**按对象授权**。
4. 在**运维用户**中选择用户等信息，单击**下一步**。



配置项	说明
授权名称	输入访问授权策略的名称。
是否启用	设置该访问授权策略是否启用。
用户	选择访问授权策略生效的用户。 ○ 选中**组授权**，表示此访问授权策略对该组中所有用户都生效。 ○ 选中部分用户，表示此访问授权策略对已选择的用户生效。

5. 在**访问范围**中选择访问目标，单击**下一步**。

   访问目标可选择指定的具体服务、主机或主机组；也可以选择一定范围内的所有主机。

   ○ 选择**对象指定**页签，选择指定的具体服务、主机或主机组。



   ■ 选中**组授权**：表示此指令授权策略对该组中所有主机都生效。

   ■ 选中**主机授权**：表示此指令授权策略对该主机中所有服务都生效。

   ■ 选中具体服务：表示此指令授权策略对选中的服务生效。

   ○ 单击**范围指定**页签，选择一定范围内的所有主机。



设置项	说明
服务器范围	在下拉栏中选择服务器合集，单击+可以选择多个服务器合集。
账号范围	选择访问服务器合集的账号范围。 ■ 选择**已定义**，表示您在**账号**中只能选择服务器合集中的主机关联的账号。 ■ 选择**自定义**，表示您在**账号**中可以选择堡垒机中创建的所有账号。
账号	选择访问服务器合集中主机所使用的账号。 ■ **所有**：**账号范围**限定内的所有账号。 ■ **指定**：选择具体账号。
服务	选择需要运维的主机服务。 ■ **所有**：**服务器范围**中所有的服务类型。 ■ **指定**：选择服务类型。

6. 在**指令集合/响应方式**中，设置指令授权的指令和响应方式，单击**保存**。



设置项	说明
配置指令集合	可配置允许或禁止使用以下指令（指令集）。
手工输入指令	可手工输入指令，多个指令请使用换行符分隔。
指令集合	在下拉栏中选择已设置好的指令集合。
响应方式	如果符合该指令规则，堡垒机的响应方式。 ○ **产生告警**：当触发该指令策略时堡垒机会生成告警事件。 ○ **阻断会话**：当触发该指令策略时堡垒机会将该会话连接中断。 ○ **忽略指令**：当触发该指令策略时堡垒机会将该指令忽略，不执行此命令并提示该指令未找到，会话可继续正常操作。 ○ **审批指令**：当触发该指令策略时会话会暂停等待管理员审批，管理员审批通过后指令会执行并可继续进行其他操作，如果管理员拒绝则指令不会执行但可以继续进行其他操作。
审批策略	可选，只有**响应方式**包含**审批指令**时需要设置。 从下拉栏中选择已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。
告警信息	可选，只有**响应方式**包含**产生告警**时需要设置。 从下拉栏中选择已设置好的告警事件。如果没有可选择的告警事件，可以从下拉栏中单击**新增**，新增告警事件。新增事件告警的操作请参见创建事件告警。

10.10.3.6.4. 配置指令授权（按访问授权）

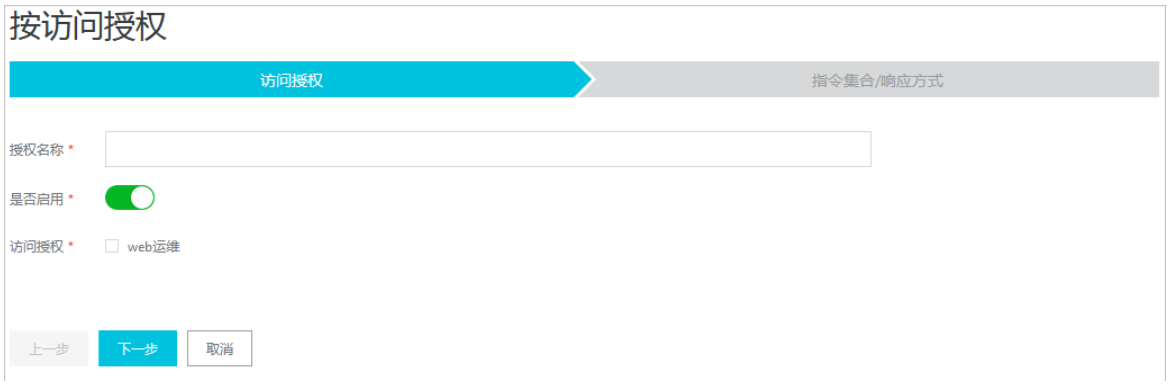
指令授权是指允许或拒绝选定的用户在目标主机上执行某些命令。按访问授权的方式，表示您直接使用访问授权中已设置的用户和目标主机。

前提条件

已创建访问授权策略，具体请参见配置访问授权。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**运维审计 > 平台侧堡垒机**。
3. 在**堡垒机**页面左侧导航栏，单击**运维管理**。
4. 在**资产管理**页面，单击**授权管理**页签。
5. 在**授权管理**页签，单击**按访问授权**。
6. 选择**访问授权**，设置授权名称和选择访问授权策略，单击**下一步**。



配置项	说明
授权名称	输入指令策略的名称。
是否启用	设置该指令授权策略是否启用。
访问授权	选择已设置的访问授权策略。

7. 在**指令集合/响应方式**中，设置指令授权的指令和响应方式，单击**保存**。



设置项	说明
配置指令集合	可配置允许或禁止使用以下指令（指令集）。
手工输入指令	可手工输入指令，多个指令请使用换行符分隔。
指令集合	在下拉栏中选择已设置好的指令集合。
响应方式	如果符合该指令规则，堡垒机的响应方式。 ○ **产生告警**：当触发该指令策略时堡垒机会生成告警事件。 ○ **阻断会话**：当触发该指令策略时堡垒机会将该会话连接中断。 ○ **忽略指令**：当触发该指令策略时堡垒机会将该指令忽略，不执行此命令并提示该指令未找到，会话可继续正常操作。 ○ **审批指令**：当触发该指令策略时会话会暂停等待管理员审批，管理员审批通过后指令会执行并可继续进行其他操作，如果管理员拒绝则指令不会执行但可以继续进行其他操作。
审批策略	可选，只有**响应方式**包含**审批指令**时需要设置。 从下拉栏中选择已设置好的审批策略。如果没有可选择的审批策略，可以从下拉栏中单击**新增**，新增审批策略。新增审批策略的操作请参见创建审批策略。

设置项	说明
告警信息	可选，只有**响应方式**包含**产生告警**时需要设置。 从下拉栏中选择已设置好的告警事件。如果没有可选择的告警事件，可以从下拉栏中单击**新增**，新增告警事件。新增事件告警的操作请参见创建事件告警。

10.10.3.7. 资源管理

10.10.3.7.1. 创建账号

该章节介绍如何创建账号。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**账号**。
4. 单击**创建**。
5. 设置账号和AD域，单击**保存**。



设置项	说明
账号	主机资源里的系统账号集合，供添加主机资源时配置账号中直接引用； -代表空账号、*代表所有账号、#代表通过堡垒机账号直接单点登录
AD域	是否为Windows AD域账号，默认为否。

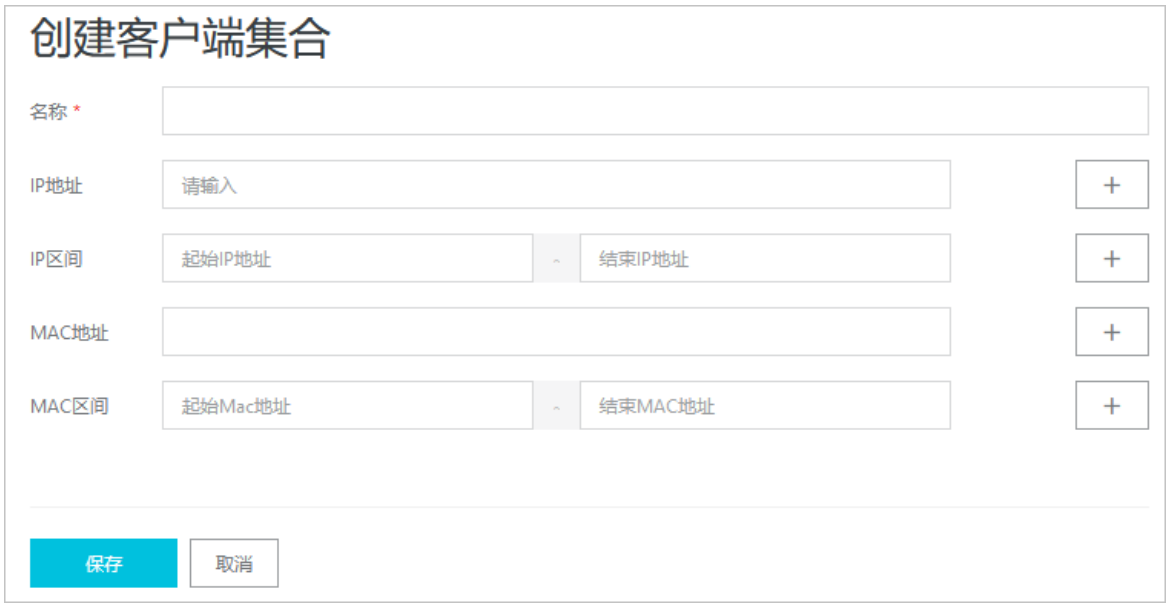
10.10.3.7.2. 创建客户端集合

在客户端集合中，您可将IP/IP区间、MAC、MAC区间配置成集合。

操作步骤

1. 登录云盾安全中心。
2.

3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**客户端集合**。
4. 单击**创建**。
5. 设置客户端集合的名称和范围，单击**保存**。



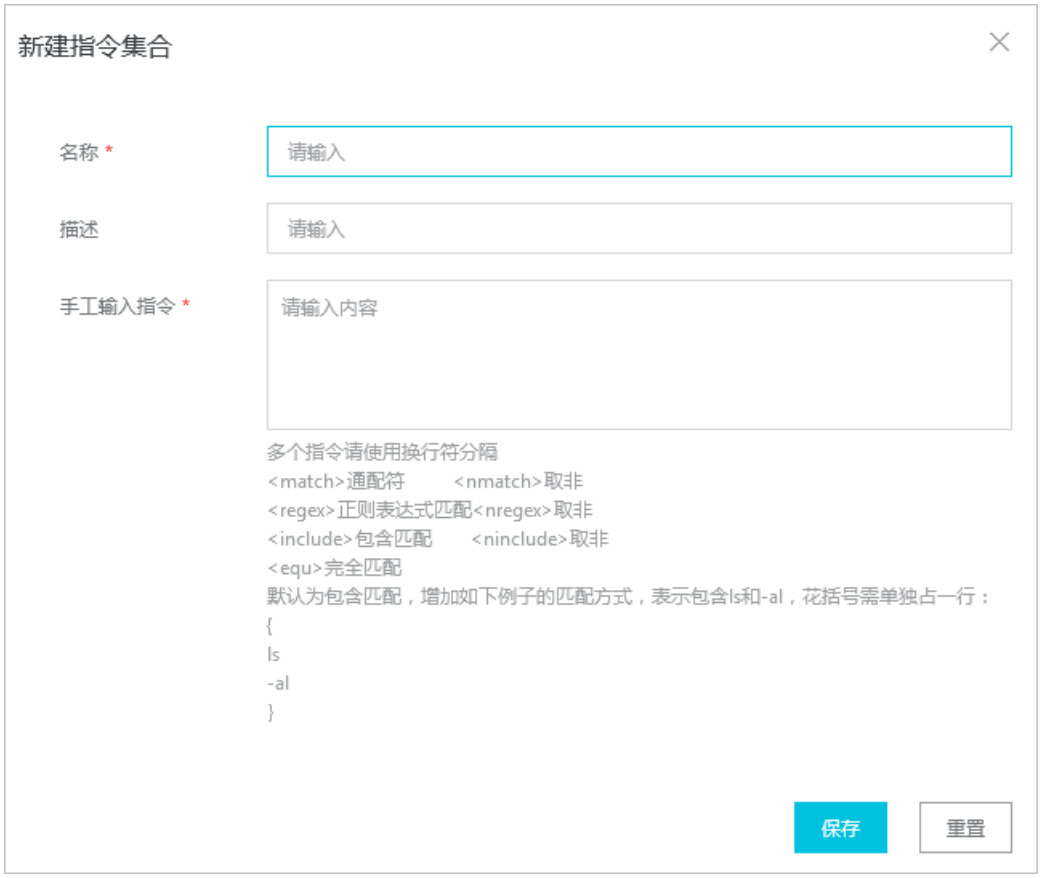
设置项	说明
名称	输入客户端集合的名称。
IP地址	设置IP地址，单击+ 可添加多个IP。
IP区间	设置IP起始和结束的范围，单击+ 可添加多个IP区间。
MAC地址	设置MAC地址，单击+ 可添加多个MAC。
MAC区间	设置MAC起始和结束的范围，单击+ 可添加多个MAC区间。

10.10.3.7.3. 创建指令集合

指令集合可将操作指令配置成集合。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**指令集合**。
4. 单击**创建**。
5. 设置指令集合，单击**保存**。



设置项	说明
名称	输入指令集合的名称。
描述	输入指令集合的详细描述信息，建议填写指令集合的用途等信息。
手工输入指令	可手工输入指令，多个指令请使用换行符分隔。

10.10.3.7.4. 创建审批策略

审批策略中可配置审批通知方式。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**审批策略**。
4. 单击**创建**。
5. 设置审批策略，单击**保存**。



设置项	说明
名称	输入审批策略的名称。
方式	选择审批通知方式，支持**消息**、**短信**和**邮件**。
短信默认	可选，只有**方式**为**短信**时需要设置。 在下拉栏中选择默认短信网关，短信网关设置请参见设置短信网关。
短信备用	可选，只有**方式**为**短信**时需要设置。 在下拉栏中选择备用短信网关，短信网关设置请参见设置短信网关。
邮件默认	可选，只有**方式**为**邮件**时需要设置。 在下拉栏中选择默认邮件服务器，邮件服务器设置请参见设置邮件。
邮件备用	可选，只有**方式**为**邮件**时需要设置。 在下拉栏中选择备用邮件服务器，邮件服务器设置请参见设置邮件。

10.10.3.7.5. 创建事件告警

事件告警中可配置违规操作、高危操作和异常登录事件的告警通知方式。

操作步骤

1. 登录云盾安全中心。

2.
3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**事件告警**。
4. 单击**创建**。
5. 设置事件告警策略，单击**保存**。



设置项	说明
名称	输入事件告警的名称。
描述	输入事件告警的描述信息。
等级	设置事件的严重等级，支持**无**、**低**、**中**和**高**。
类型	选择事件的类型，支持**无**、**违规操作**、**高危操作**和**登录异常**。
方式	选择告警通知方式，支持**无**、**邮件**和**短信**。
默认	可选，只有**方式**为**邮件**或**短信**时需要设置。 在下拉栏中选择默认邮件或短信网关。 ○ 邮件服务器设置请参见设置邮件。 ○ 短信网关设置请参见设置短信网关。

设置项	说明
备用	可选，只有**方式**为**邮件**或**短信**时需要设置。 在下拉栏中选择备用邮件或短信网关。 ○ 邮件服务器设置请参见设置邮件。 ○ 短信网关设置请参见设置短信网关。 ○

10.10.3.7.6. 创建服务器集合

在服务器集合中，您可将运维主机或主机组配置成集合。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**服务器集合**。
4. 单击**创建**。
5. 设置服务器集合的名称和范围，单击**保存**。



设置项	说明
名称	输入服务器集合的名称。
IP限制	是否启用IP限制功能，启用后集合只包括指定IP范围内的主机。 ○ **IP地址**：设置IP地址，单击+可添加多个IP。 ○ **IP区间**：设置IP起始和结束的范围，单击+可添加多个IP区间。

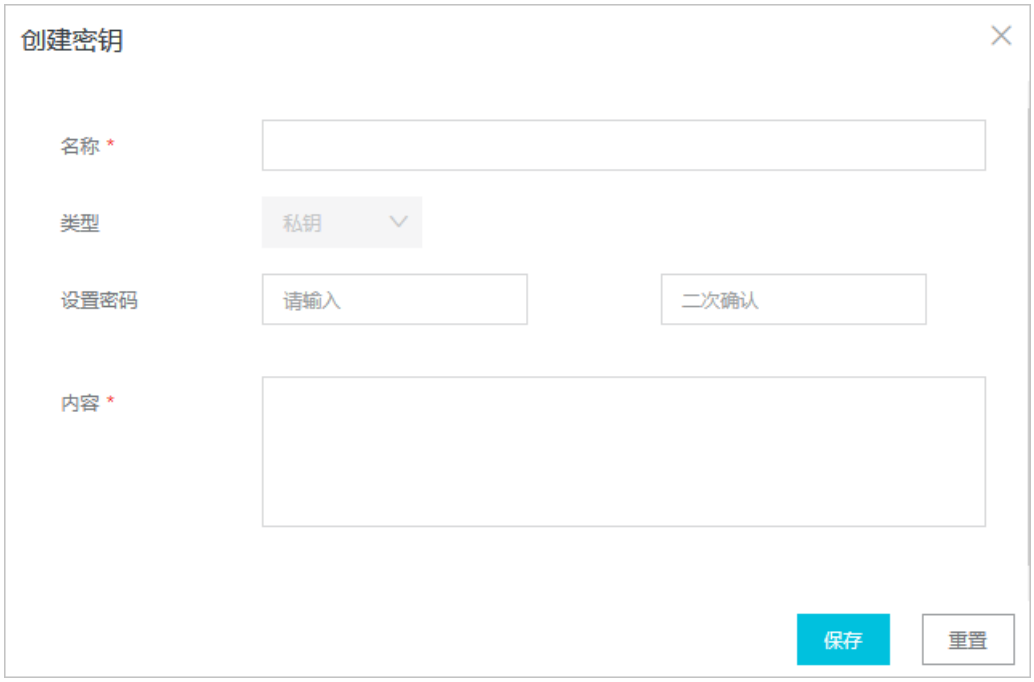
设置项	说明
主机	选择服务器集合中包含的主机或主机组。 ○ 选中**组授权**：表示选择该主机组下所有主机。 ○ 选中具体主机：表示选择已选中的主机。

10.10.3.7.7. 创建密钥

在密钥管理中，您可以添加SSH认证私钥，用于堡垒机通过密钥方式登录被运维主机。已创建私钥可通过密码录入下发给指定主机账号。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**运维管理**，在**资产管理**的**资源管理**页签，单击**密钥管理**。
4. 单击**创建**。
5. 设置密钥名称和内容，单击**保存**。



设置项	说明
名称	输入密钥的名称。
类型	固定为**私钥**。

设置项	说明
设置密码	可选，为私钥设置密码并确认密码。 **说明** 如果需要密钥方式免密登录，则此处密码设置为空。
内容	输入私钥内容。

10.10.3.8. 系统管理

10.10.3.8.1. 设置Web登录超时时间

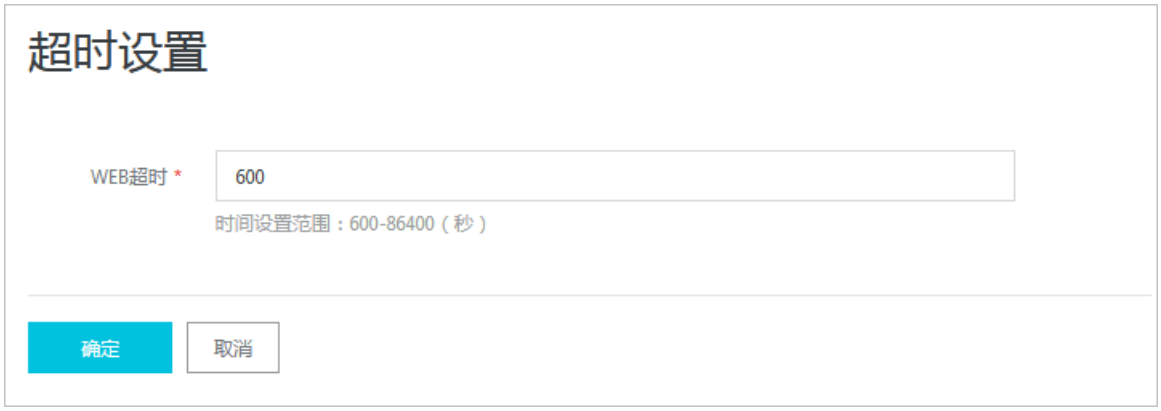
本文介绍如何设置用户登录堡垒机Web页面的超时时间。

背景信息

如果您登录堡垒机的Web管理页面后，在超时时间内没有任何操作，您的账号将自动退出。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，单击**系统管理**，在**系统管理**页面单击**超时设置**。
4. 输入**WEB超时**的时间，单击**确定**。



10.10.3.8.2. 设置对外输出方式

该章节介绍堡垒机的对外输出方式，支持邮件、短信网关和FTP等模式。

设置邮件

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，单击**系统管理**，在**系统管理**页面单击**输出设置**。
4. 在**邮件**页签，单击**创建**。

5. 在**创建邮件配置**对话框中，设置邮件发送信息。



参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
服务器地址	发送邮件服务器地址。
端口	发送邮件服务器端口。
连接方式	支持的连接方式包括*加密*和*非加密*。
发送邮箱地址	发送邮件的邮箱账号。
服务器账号	账号信息。
服务器验证	邮箱账号登录是否需要验证。
附件大小	邮件发送附件的最大值。
编码方式	邮件服务器编码格式，支持*UTF-8*和*GBK*。
方式	配置该邮件服务器为默认发送服务器或备用发送服务器。
测试	测试邮件服务器是否能够正常发送。 在输入框中输入接收邮箱账号，单击**测试**。

6. 单击**保存**。

设置短信网关

1. 登录云盾安全中心。

2. 单击**运维审计 > 平台侧堡垒机 > 系统管理**。
3. 单击**输出设置**。
4. 在**短信网关**页签，单击**创建**。
5. 在**创建短信配置**对话框中，设置短信网关参数。根据短信网关的类型，支持配置**数据库短信网关**和**阿里云短信网关**。



- 数据库短信网关

参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
短信网关类型	在下拉框中选择*数据库短信网关*。
数据库类型	在下拉框中选择数据库类型，支持*ORACLE*、*MSSQL*、*MYSQL*和*SYBASE*。
服务器地址	填写数据库服务器地址。
端口	填写数据库服务器端口。
账号	填写数据库账号
密码	填写数据库密码。
数据库	填写数据库名。
短信sql语句模板	插入的SQL语句模板。
编码方式	短信内容的编码格式，支持*UTF-8*和*GBK*。
方式	配置该服务器为默认发送服务器或备用发送服务器。
测试	测试服务器是否能够正常发送。

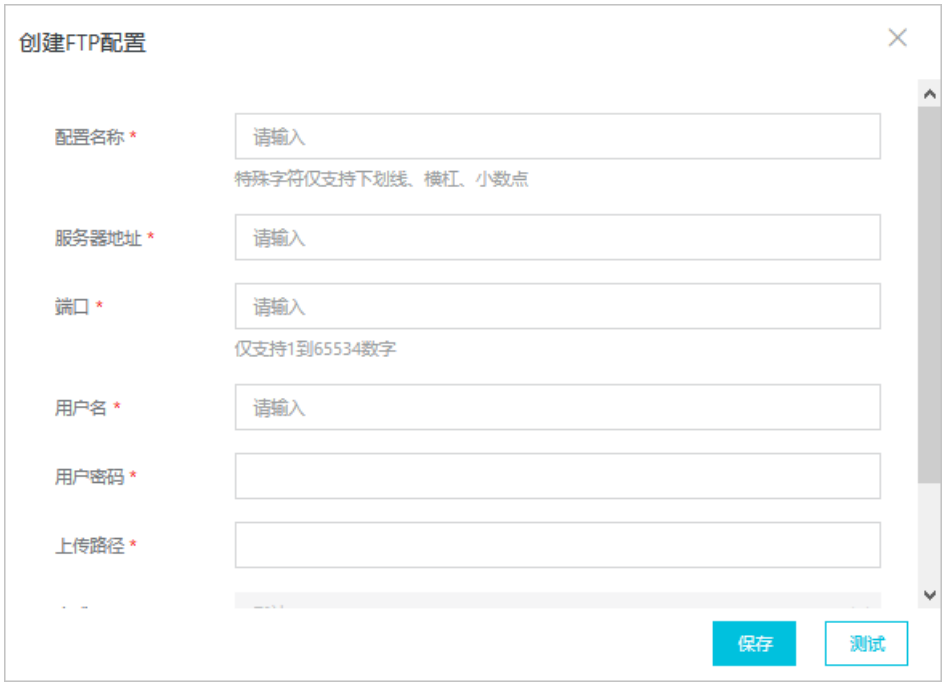
- 阿里云短信网关

参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
短信网关类型	在下拉框中选择*阿里云短信网关*。
密钥ID	填写账号密钥ID。
密钥	填写账号密钥。
区域ID	填写区域ID。
签名	填写短信签名。
模板	填写短信模板ID。
参数	填写短信模板中用到的模板变量名称。
编码方式	短信内容的编码格式，支持*UTF-8*。
方式	配置该服务器为默认发送服务器或备用发送服务器。
测试	测试服务器是否能够正常发送。

6. 单击**保存**。

设置FTP

1. 登录云盾安全中心。
2. 单击**运维审计 > 平台侧堡垒机 > 系统管理**。
3. 单击**输出设置**。
4. 在**FTP**页签，单击**创建**。
5. 在**创建FTP配置**对话框中，设置FTP参数。



参数	说明
配置名称	配置备注名称，便于您识别和后续维护。
服务器地址	填写FTP服务器地址。
端口	填写FTP服务器端口。
用户名	填写FTP账号。
用户密码	填写FTP密码。
上传路径	填写上传FTP的指定文件夹路径。
方式	配置该服务器为默认发送服务器或备用发送服务器。
模式	FTP的传输模式，支持*被动*和*主动*。

6. 单击**保存**。

10.10.3.9. 密码管理

10.10.3.9.1. 密码录入

通过密码录入，您可以为指定的主机账号统一设置密码、密钥。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，选择**密码管理**。

4. 在**密码管理**页签，单击**密码录入**。
5. 选择主机账号并设置主机账号对应的**密码**和**密钥**，单击**保存**。



设置项	说明
主机	选择要录入的密码或密钥对应的主机账号。
密码	可选，只有选中后才会生效。 输入并确认主机账号对应的密码。选中**空密码**表示设置空密码。
密钥	可选，只有选中后才会生效。 从已创建的密钥中选择主机账号对应的密钥。如果没有创建过密钥，您可以选择**新增**并创建密钥。创建密钥的操作请参见创建密钥。

6. （可选）如果选择了多个主机账号，根据页面提示确认统一修改密码。



执行结果

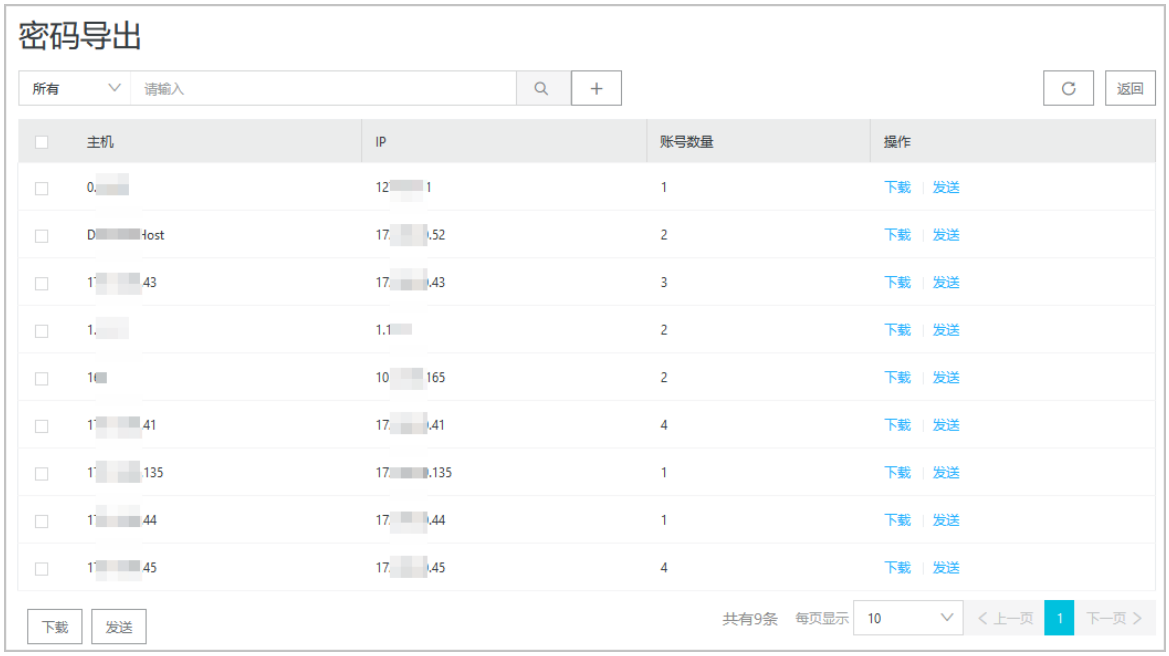
页面提示保存成功，表示成功录入密码。

10.10.3.9.2. 密码导出

通过密码导出，您可以将指定主机账号的密码下载到本地或发送给管理员。

操作步骤

1. 登录云盾安全中心。
2.
3. 选择**运维审计 > 平台侧堡垒机 > 密码管理**。
4. 在**密码管理**页签，单击**密码导出**。
5. 选中目标主机并选择**下载**或**发送**主机账号的密码。



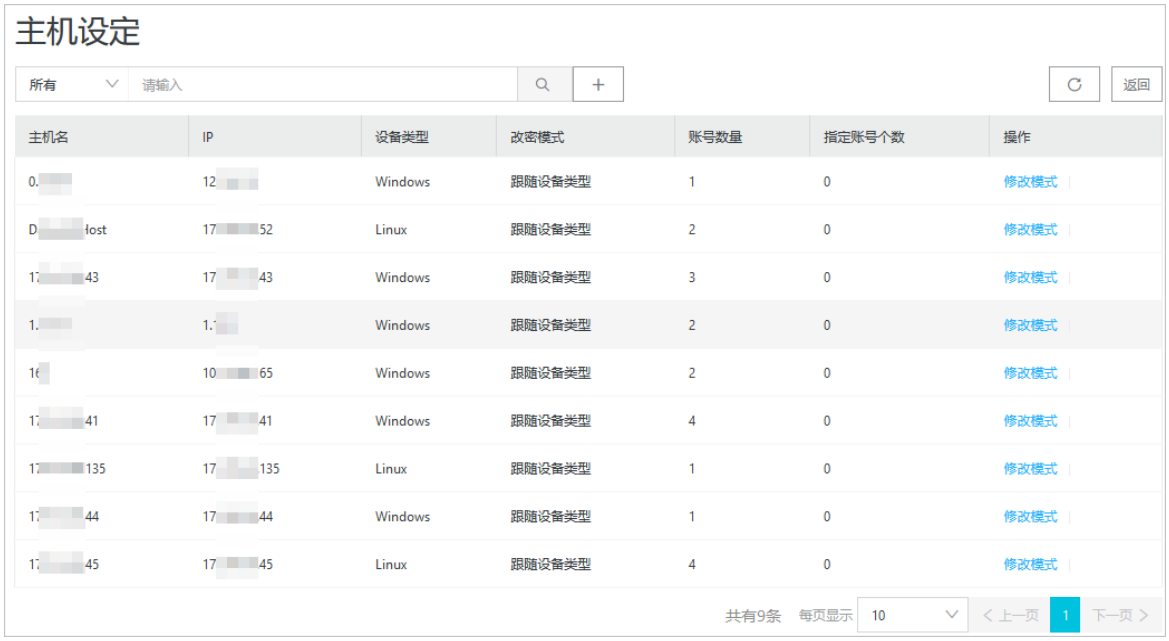
- **下载**：下载主机账号密码文件。下载的密码文件需要通过密码查看器查看。
- **发送**：将主机账号的密码文件通过设定的发送方式发送给管理员。

10.10.3.9.3. 主机设定

通过主机设定，您可以设定运维主机和账号的改密模式。

操作步骤

1. 登录云盾安全中心。
2.
3. 选择**运维审计 > 平台侧堡垒机 > 密码管理**。
4. 在**密码管理**页签，单击**主机设定**。
5. 定位到要操作的主机，单击其操作列下的**修改模式**。



6. 在**主机**页签，设置主机改密模式，并单击**保存**。

设置项	说明
改密方式	默认为**跟随设备类型**，支持选择**自定义**。
改密配置	默认为主机对应设备类型的默认改密配置，例如主机设备类型为Windows，则改密配置默认为**Windows改密配置**。支持选择**新增**，并自定义改密配置的名称。
改密脚本	使用默认改密配置时，改密脚本为**默认**且不可修改。 使用自定义改密配置时，支持使用**默认**改密脚本或选择**自定义**，自定义改密脚本。
脚本	仅在**改密脚本**为**自定义**时需要配置。 输入自定义改密脚本。
连接方式	仅在**改密脚本**为**默认**时需要配置。 选择改密配置的连接方式。

7. 选择**账号**页签，单击账号操作列下的**修改模式**，自定义账号改密模式。



账号的**改密方式**默认为**跟随主机**。您可以参照自定义主机改密模式的操作，自定义账号改密模式。

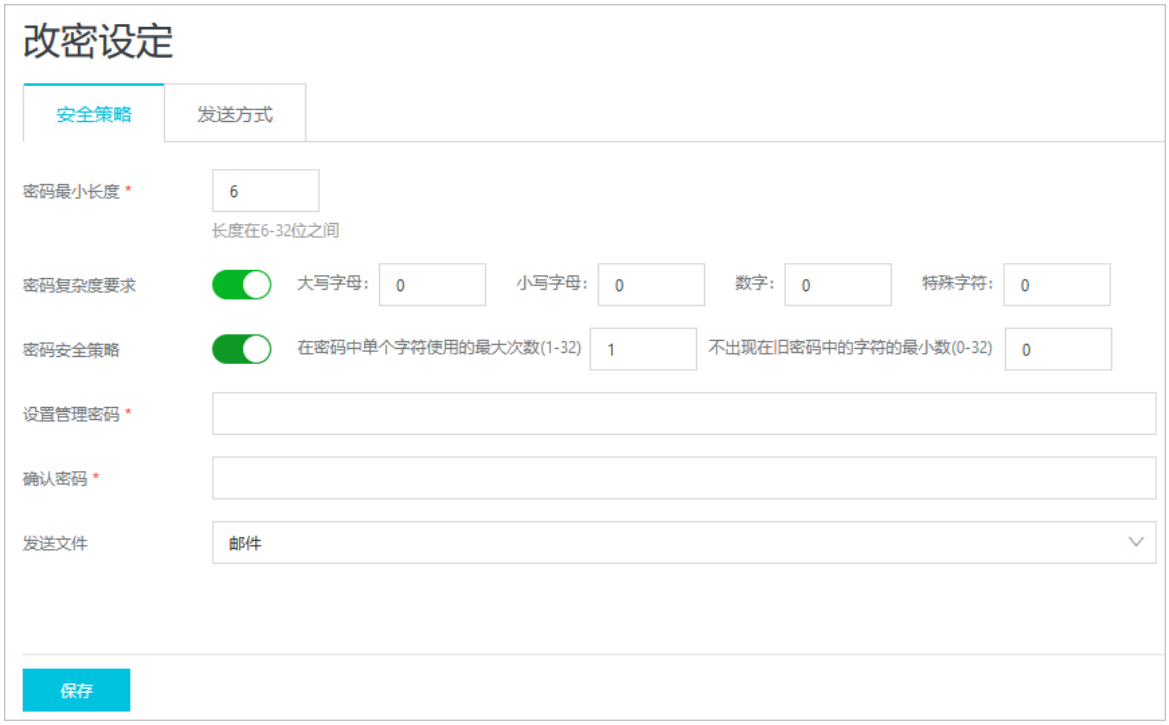


10.10.3.9.4. 改密设定

通过改密设定，您可以配置自动改密时密码的生成规则和发送方式。

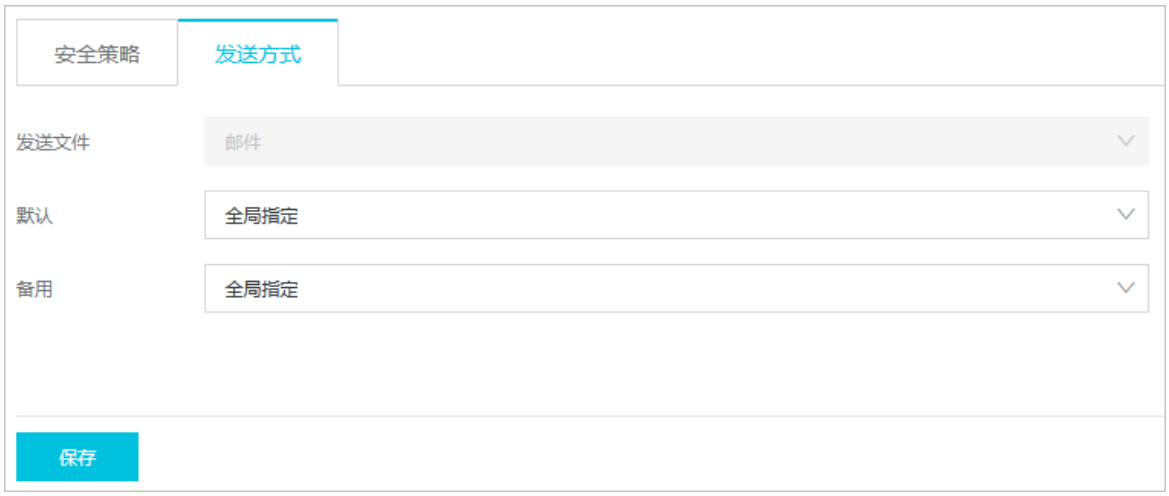
操作步骤

1. 登录云盾安全中心。
2.
3. 选择**运维审计 > 平台侧堡垒机 > 密码管理**。
4. 在**密码管理**页签，单击**改密设定**。
5. 在**安全策略**页签，配置自动改密时密码的生成规则，单击**保存**。



设置项	说明
密码最小长度	设置改密时随机生成密码的最小长度。
密码复杂度要求	开启后，可以设置改密时随机生成密码必须包含的字符类型及位数。支持的字符类型包括**大写字母**、**小写字母**、**数字**、**特殊字符**。
密码安全策略	开启后，可以设置改密时随机生成密码最多允许出现的重复字符的个数。具体支持以下配置项： ○ **在密码中单个字符使用的最大次数** ○ **不出现在旧密码中的字符的最小数**
设置管理密码	为密码文件设置查看密码。
确认密码	确认密码文件的查看密码。
发送文件	设置密码文件的发送方式，可选值：**邮件**、**FTP**。

6. 选择**发送方式**页签，配置密码文件的发送方式，单击**保存**。



支持邮件和FTP两种方式，**发送文件**固定为步骤4中设置的**发送文件**方式。

- **发送文件**为**邮件**时，可以选择已设置的邮件发送方式，默认为**全局指定**。创建邮件发送方式的操作请参见设置邮件。
- **发送文件**为**FTP**时，可以在选择已设置的FTP发送方式，默认为**全局指定**。创建FTP发送方式的操作请参见设置FTP。

10.10.3.9.5. 自动改密

通过自动改密，您可以创建并管理自动改密计划。

前提条件

已完成改密设定。更多信息，请参见改密设定。

操作步骤

1. 登录云盾安全中心。

2.
3. 选择**运维审计 > 平台侧堡垒机 > 密码管理**。
4. 在**密码管理**页签，单击**自动改密**。
5. 在**改密对象配置**中，设置改密计划的名称和对象，单击**下一步**。



设置项	说明
名称	填写改密计划的名称。特殊字符仅支持下划线（_）、短横杠（-）和小数点（.）。
发送预备改密文件	是否发送预备改密文件。开启后，则自动改密计划执行前会发送预改密密码，管理员收到文件后，需要在堡垒机消息中确认，自动改密计划才会继续执行。

设置项	说明
改密对象	通过**对象指定** 或**范围指定**方式指定要修改密码的主机账号。 ○ **对象指定**：直接选中具体的主机账号。 ■ 选中**组托管**：表示选中该组主机下的所有账号。 ■ 选中**主机托管**：表示选中该主机下的所有账号。 ○ **范围指定**：选择一定范围内主机下的账号。 ■ **服务器范围**：选择已定义的服务器合集，单击+可以选择多个服务器合集。 ■ 账号范围：选择访问服务器合集的账号范围。 ■ 选择**已定义**，则在**账号**中只能选择服务器合集中的主机关联的账号。 ■ 选择**自定义**，则在**账号**中可以选择堡垒机中创建的所有账号。 ■ **账号**：选择访问服务器合集中主机所使用的账号。 ■ **所有**：**账号范围**限定内的所有账号。 ■ **指定**：选择具体账号。 ■ **服务**：选择需要用到的主机服务。 ■ **所有**：**服务器范围**中所有的服务类型。 ■ **指定**：选择具体服务类型。

6. 在**改密策略配置**中，设置改密计划的开始时间和重复周期等信息，单击**保存**。



设置项	说明
策略名称	可选。从下拉栏中选择**新增**可将配置信息保存为模板，方便后续直接引用模板。添加新策略时需要设置策略名称。
开始时间	设置改密计划的开始执行时间。
重复周期	设置重复执行当前改密计划的周期，单位为**天**或**分钟**。

设置项	说明
密码策略	设置自动改密计划的密码生成策略，可选项： ○ **随机生成不同密码** ○ **随机生成相同密码** ○ **人工指定相同密码**：使用该策略时，必须设置密码。
发送方式	选择密码发送方式，支持**邮件**与**FTP**方式。默认使用改密设定中指定的方式。

执行结果

成功创建自动改密计划后，页面跳转到**自动改密**管理页面。您可以在此查看改密计划的执行状态和结果，并根据需要停用/启用改密计划、修改改密计划、删除改密计划。



10.10.3.9.6. 手工改密

通过手工改密，您可以统一修改指定主机账号的密码。

操作步骤

1. 登录云盾安全中心。
2.
3. 选择**运维审计 > 平台侧堡垒机 > 密码管理**。
4. 在**密码管理**页签，单击**手工改密**。
5. 选择要改密的**主机**账号，设置并确认**新密码**，单击**执行**。



执行结果

手工改密任务直接执行并返回改密结果。

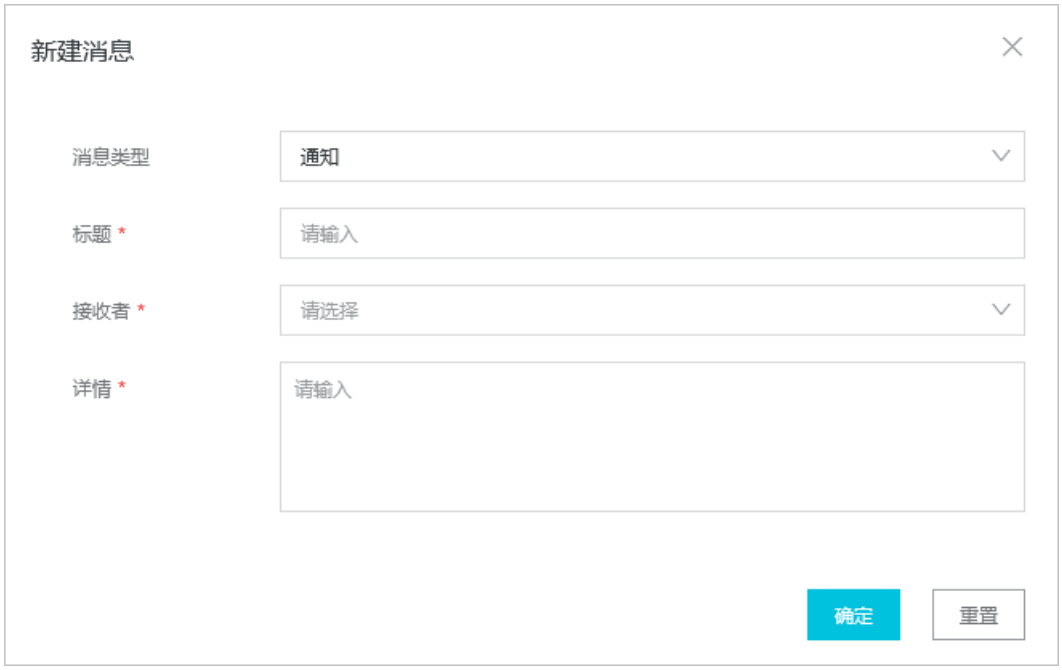
10.10.3.10. 消息中心

10.10.3.10.1. 发送消息

本文介绍如何在堡垒机中给其他用户发送消息。

操作步骤

1. 登录云盾安全中心。
2.
3. 在**堡垒机**页面左侧导航栏，单击**消息中心**。
4. 在**发送**页签，单击**新建消息**。
5. 选择消息类型并填写消息，单击**确定**，发送消息。



消息项	说明
消息类型	在下拉框中选择消息类型，仅支持**通知**。
标题	输入消息的标题。
接收者	在下拉框中选择消息接收人，可选择多个人员群发消息。
详情	输入消息的详细信息。

10.10.3.10.2. 查看消息

在消息中心查看接收到的消息。

操作步骤

1. 登录云盾安全中心。
2.
3. 在左侧导航栏，单击**消息中心**。
4. 在**接收**页签的消息列表中查看信息。

10.10.4. 运维员操作指南

10.10.4.1. 登录堡垒机运维环境

该章节介绍运维人员如何登录堡垒机的运维环境。

前提条件

- 管理员已经为运维人员创建用户并设置运维访问授权。

- 运维人员已从管理员处已获取平台侧堡垒机运维地址。

此步骤由运维人员操作，登录堡垒机运维环境，具体操作如下：

1. 在浏览器地址栏中，输入平台侧堡垒机运维管理系统的访问地址，按回车键。

   堡垒机的登录格式如下：

   ```
   https://<平台侧堡垒机运维管理系统访问地址>
   ```

2. 输入正确的用户名和密码，单击**登录**。

   > **说明** 运维人员的用户名和密码请从管理员处获取。

10.10.4.2. 安装运维客户端

在使用堡垒机运维前，需要安全运维客户端（Bhost Client）。本章节介绍如何安装Bhost Client。

操作步骤

1. 登录堡垒机运维环境。
2. 使用admin账号登录运维管理系统页面。
3. 单击**访问工具 > 相关下载**。
4. 在**相关下载**页面，单击**Bhost Client**，将客户端文件（*BHost Client.exe*）下载到本地。
5. 在本地主机中，双击*BHost Client.exe*，根据提示默认安装完运维客户端。

10.10.4.3. 通过Web方式运维

本章节介绍运维人员如何在堡垒机中通过Web方式运维主机。

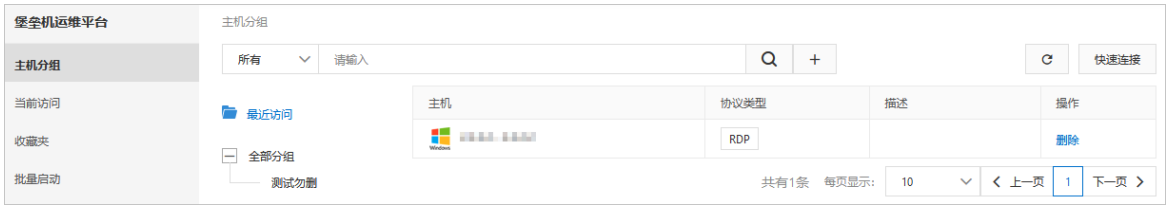
背景信息

通过Web方式运维支持RDP、SSH、SFTP等常用协议，本章节以RDP为例。

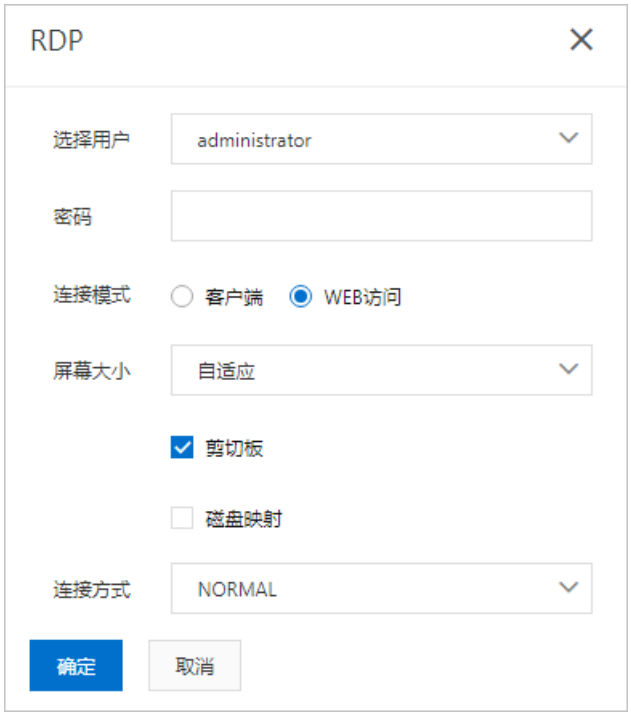
操作步骤

1. 登录堡垒机运维环境。

2. 在左侧导航栏中单击**主机分组**。



3. 在**全部分组**中，单击目标主机所在的分组。
4. 在主机列表的**协议类型**列，单击运维协议（例如**RDP**）。
5. 在登录对话框中，设置登录信息，单击**确定**。



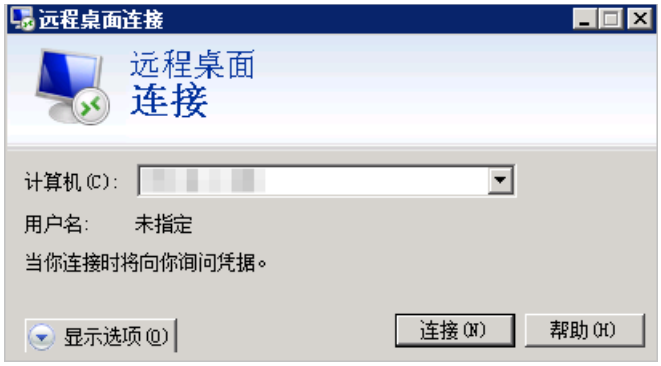
   - 在**选择用户**选择登录主机的账号。
   - 在**密码**中输入主机账号的登录密码。
   - 在**连接模式**中选择运维模式，此步骤选择**WEB访问**。

10.10.4.4. 通过客户端方式运维

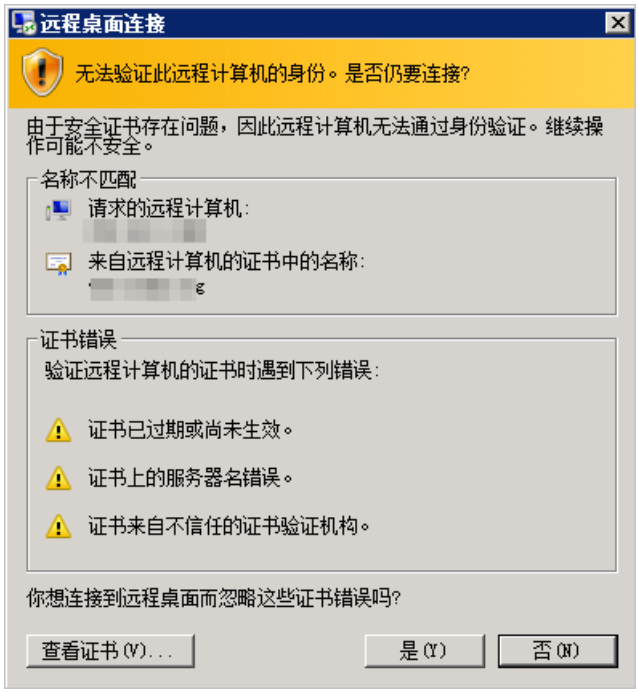
本章节介绍通过客户端方式运维主机，包括RDP协议、SFTP协议和SSH协议运维。

RDP协议运维

1. 运维人员在本地主机打开远程桌面连接工具（Mstsc）。
2. 输入堡垒机运维地址，单击**连接**。



3. 在**远程桌面连接**提示框中，单击**是**。



4. 在堡垒机**登录**窗口，输入运维人员的账号和密码，单击**确定**。

> **说明** 运维人员的账号和密码请从管理员处获取。

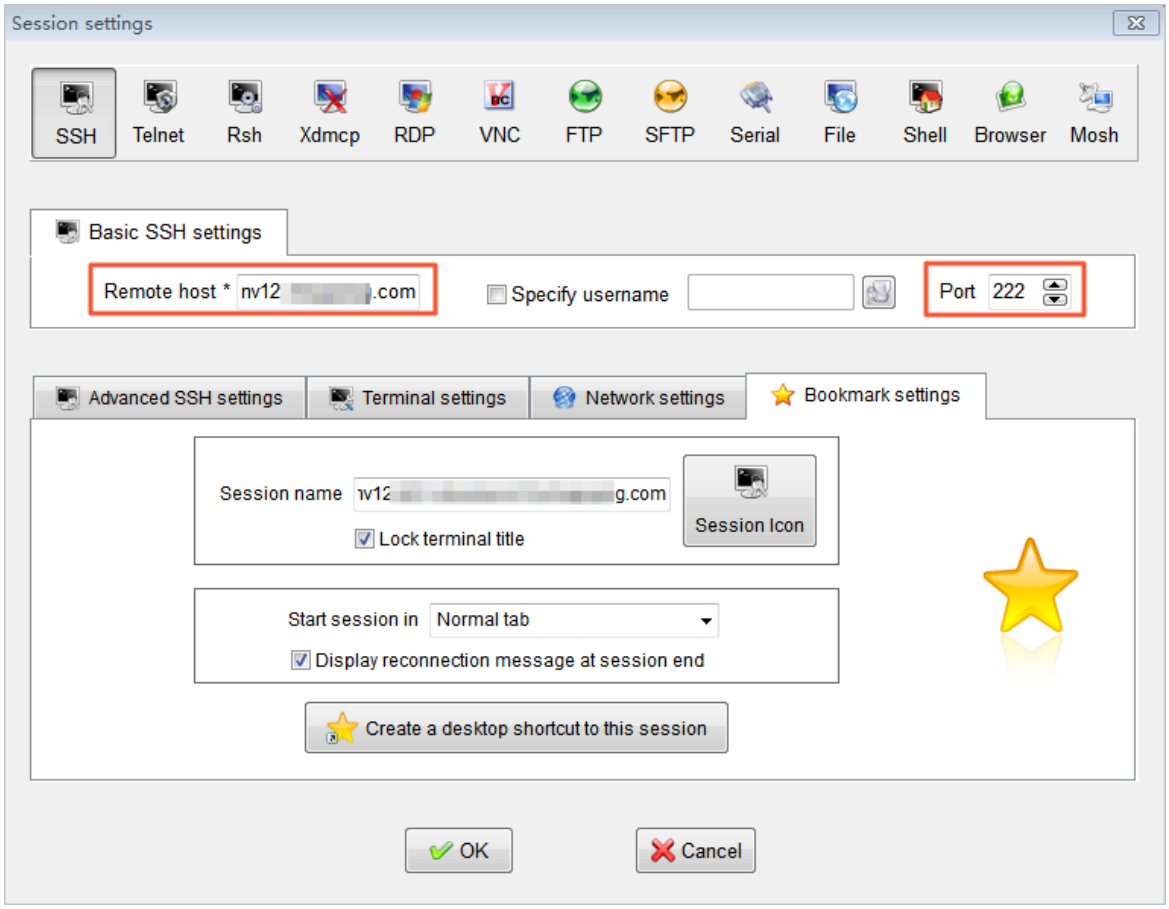


5. 选择运维主机的**设备**、**主机服务**和**账号**，单击**确定**登录主机。



SSH协议运维

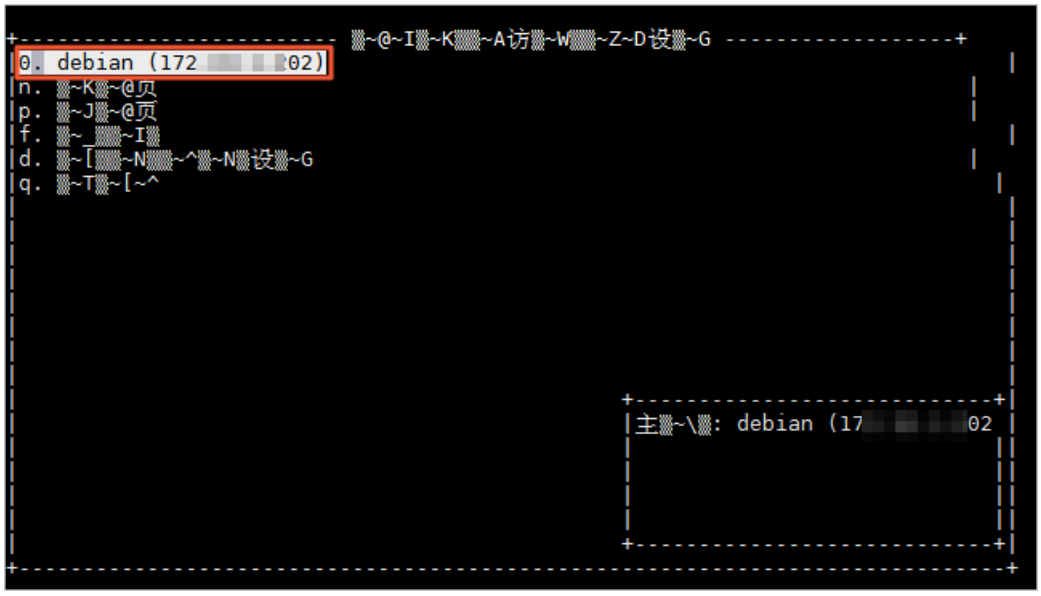
1. 运维人员在本地主机打开SSH连接工具（例如MobaXterm）。
2. 输入堡垒机的运维地址和端口号（222），单击**OK**。



3. 输入运维人员的堡垒机账号，按回车键（Enter），再输入密码，按回车键（Enter）。



4. 通过上、下方向键依次选择主机组、主机、协议（SSH）和主机账户，按回车键（Enter）。



5. 输入账户密码，按回车键（Enter），登录目标主机。

10.11. 安全编排自动化响应

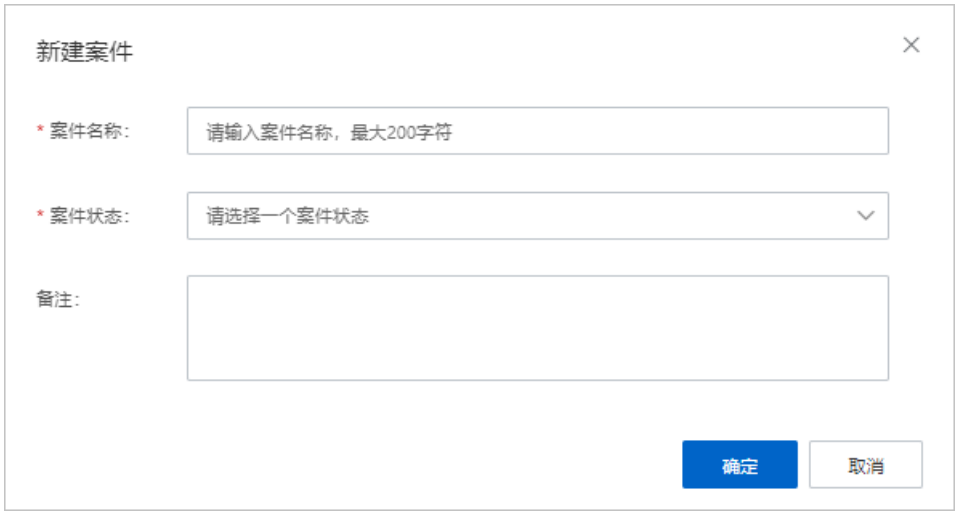
10.11.1. 事件调查

10.11.1.1. 案件管理

案件包括SOC告警事件和用户手动创建的案件。本文介绍了如何创建案件、查看案件信息、调查案件、查看案件统计情况。

创建案件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>案件管理**。
5. 在**案件管理**页签，单击**新建**。
6. 在**新建案件**对话框，配置案件的基本信息。



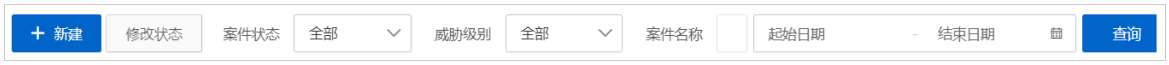
配置项	说明
案件名称	输入需要新建的案件名称。
案件状态	单击下拉列表，选择该案件所处的状态。可选状态有：**新建**、**调查中**、**待处置**、**监控中**、**已处置**、**忽略**。
备注	设置案件备注信息。

7. 单击**确认**。
   新建好的案件显示在**案件管理**页面的案件列表中。

查看案件信息

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>案件管理**。
5. 在**案件管理**页签下，查看全部案件。

   您还可以参考下表设置搜索项，搜索安全事件。



搜索项	说明
案件状态	选择案件目前的状态。
威胁级别	选择案件的威胁级别。
案件名称	输入案件的名称。
起始日期	设置案件查询的起始日期。
结束日期	设置案件查询的结束日期。

6. 在案件列表中查看案件基础信息。

   案件列表按照时间倒序展示最新的案件信息。



   单击案件行的**详情**，在**详情**页面上方，您可以查看案件的具体信息。

   在案件列表页面，您还可以进行如下操作。

   - 查询案件：支持通过选择**案件状态**、选择**威胁级别**、输入**案件名称**、设置**起始日期**和**结束日期**进行查询。



   - 删除案件：单击指定案件的**删除**，即可在情报列表中删除选定案件。
   - 快速设置案件状态为已处置：单击指定案件的**设为已处置**，即可将**案件状态**列显示为**已处置**。
   - 修改案件状态：选中指定案件前的复选框，单击**修改状态**，在**修改状态**对话框选择您要修改的状态，可选择：**新建**、**调查中**、**待处置**、**已处置**、**忽略**、**监控中**。

调查案件

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>案件管理**。
5. 在**案件管理**页面，单击**详情**。
6. 在**详情**页面，调查案件。

   当安全事件发生时，系统可以在第一时间将安全事件加入到作战室中，并开始案件的调查处置，案件相关的信息会显示在作战室中。安全分析员可以将事件中的相关恶意指标加入情报中持续监控。通过响应记录则能看到在事件调查和响应过程中执行过的所有操作的记录。

i. 单击**联合作战室**，在**联合作战室**页签的消息文本框内输入指令，单击**发送**。



您可以在**响应动作**页面下，查看可以给机器人发送的指令，页面所列的**名称**为指令。

您在输入框中输入**@贾维斯**和指令发送后，可以对机器人发送指令。您在输入框中@其他成员，可以对其他人发送消息。

群成员可以支持多人在联合作战室中协同工作，发送消息、共享安全告警信息和事件调查的结果，实现安全事件的协同处置。

ii. 单击**相关指标**，在**相关指标**页签下，查看案件的相关实体，对实体处置状态保持跟踪。



实体是指某一种固定类型的数据，此处实体类型有：

服务器IP、主机名、应用名、域名、数据库、cna、文件hash、进程、AccesskeyID、邮箱、Aegis文件、文件MD5。

iii. 单击**响应记录**，在**响应记录**页签下，查看在案件件调查和响应过程中执行过的所有操作的记录。



响应记录是机器人在联合作战室响应指令的执行记录。执行记录会按时间顺序展示，最近的一次执行记录会显示在最上方。

查看案件统计情况

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>案件管理**。
5. 在**案件管理**页签下，查看案件统计情况。

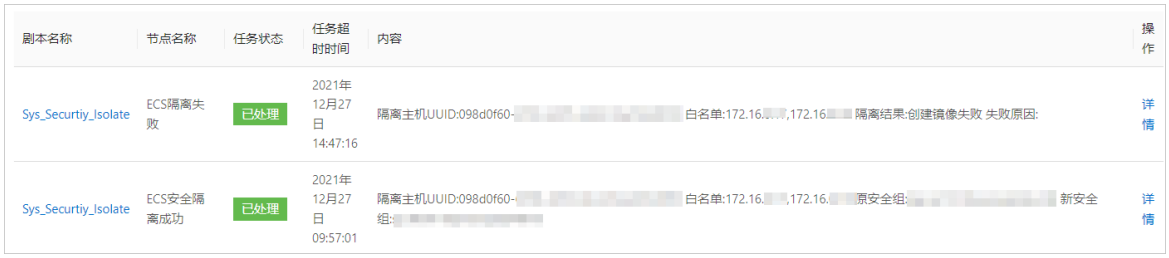


- **新增案件数**：用于统计当前阿里云账号新增的案件数。
- **待处置案件**：当前阿里云账号需要安全管理员关注和进一步处理的案件的数量。
- **自动响应案件数**：展示当前阿里云账号统计周期内自动响应的案件数量。
- **自动封禁威胁数**：展示当前阿里云账号今天、本周已经通过剧本自动封禁的威胁数量。

10.11.1.2. 任务列表

本文介绍了如何查看**任务列表**页面的剧本任务信息。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>任务列表**。
5. 在**任务列表**页面，设置搜索条件，单击**查询**。
6. 在**任务列表**页面，查看任务详细信息。



- **剧本名称**：自动化编排剧本的名称。
- **节点名称**：剧本任务节点的名称。
- **任务状态**：当前任务的状态。
- **任务超时时间**：任务处理的超时时间。
- **内容**：任务的具体内容。
- **操作**：可以对任务进行查看**详情**的操作。单击**详情**，进入**案件管理**页面。

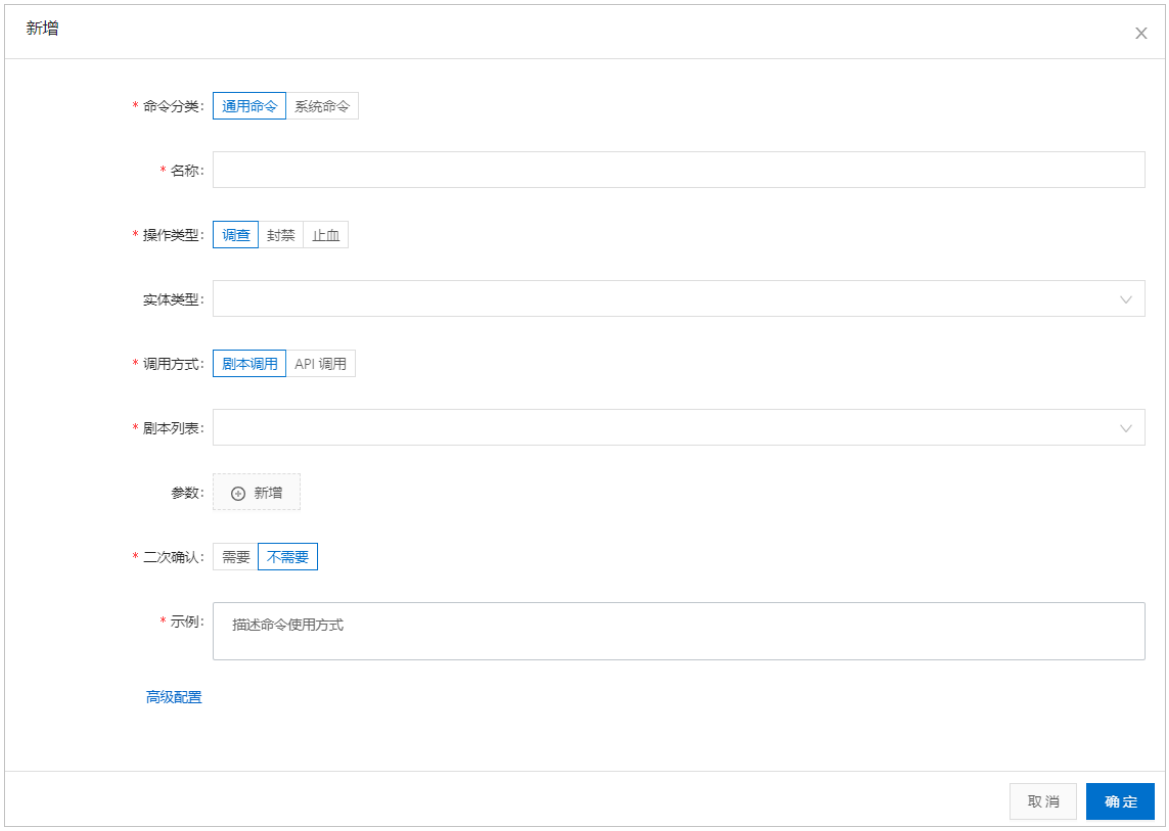
在**任务列表**页面，您还可以在**剧本名称**列，单击剧本名称，进入**剧本列表**页面。

10.11.1.3. 响应动作

本文介绍了如何创建响应动作和查看响应动作信息。

创建响应动作

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>响应动作**。
5. 在**响应动作**页面，单击**新增**。
6. 在**新增**对话框，设置动作参数。



参数	说明
命令分类	响应动作的命令分类。可选值有：**通用命令**、**系统命令**。
名称	响应动作的名称。
操作类型	响应动作的操作类型，可选值有：**调查**、**封禁**、**止血**。
实体类型	响应动作的实体类型，可选值有：**服务器IP**、**Aegis文件**。
调用方式	任务的调用方式，有**剧本调用**和**API调用**两种方法。当选择**剧本调用**时，需要配置**剧本列表**参数，当选择**API调用**时，需要配重**Bean名称**参数。

参数	说明
剧本列表	在下拉列表中选择剧本列表中的剧本。
（可选）参数	单击 新增 图标，设置Key、Value。
二次确认	设置是否需要二次确认，可选择**需要**、**不需要**。
示例	描述命令的使用方式。

7. 单击**确定**。
   在动作列表中显示新增的响应动作。

查看响应动作信息

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>事件调查>响应动作**。
5. 在**响应动作**页面，在文本框输入响应动作的**名称**、**描述**或**示例**，单击搜索图标。
   您可以通过响应动作的**名称**、**描述**、**示例**筛选响应动作。
6. 在响应动作列表，查看响应动作的信息。



ID	名称	描述	示例	最后修改	操作
58	重保巡检	通用命令	测试	(2021-12-23 17:56:51)	编辑 删除
59	巡检恶意IP	通用命令	测试	(2021-12-23 18:09:56)	编辑 删除
55	全网封禁	通用命令	测试	(2021-12-23 21:33:29)	编辑 删除
60	test54	通用命令	44	(2021-12-27 21:06:02)	编辑 删除
56	ban_whole-ban	通用命令	一键封禁功能	(2021-12-27 14:46:17)	编辑 删除
51	解封实体	系统命令	系统命令	(2021-10-27 15:07:19)	编辑 删除

   - **ID**：响应动作的ID。
   - **名称**：响应动作的名称。
   - **描述**：响应动作命令分类的描述。有：**通用命令**和**系统命令**两种描述。
   - **示例**：命令使用方式的描述。
   - **最后修改**：响应动作最后修改的用户和时间。
   - **操作**：可以对响应动作进行**编辑**和**删除**操作
     - 编辑响应动作：单击**编辑**，您可以在**编辑**对话框，修改响应动作的参数。
     - 删除响应动作：单击**删除**，在**确认删除吗？**对话框单击**确定**，可以删除所在行的响应动作。

10.11.2. 自动化编排

10.11.2.1. 剧本管理

本文介绍了如何查看剧本列表和管理剧本。

背景信息

自动化编排目标是将安全运营日常工作自动化、流程化，提升安全响应速度，简化安全专家的日常工作，集中精力对抗高级持续攻击APT（Advanced Persistent Threat）。安全运营的日常工作可沉淀为可视化、可解释、可执行的剧本沉淀在产品内，更利于运营经验的传承。

查看剧本列表

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>自动化编排>剧本列表**。
5. 在**剧本列表**页面，查看剧本信息。



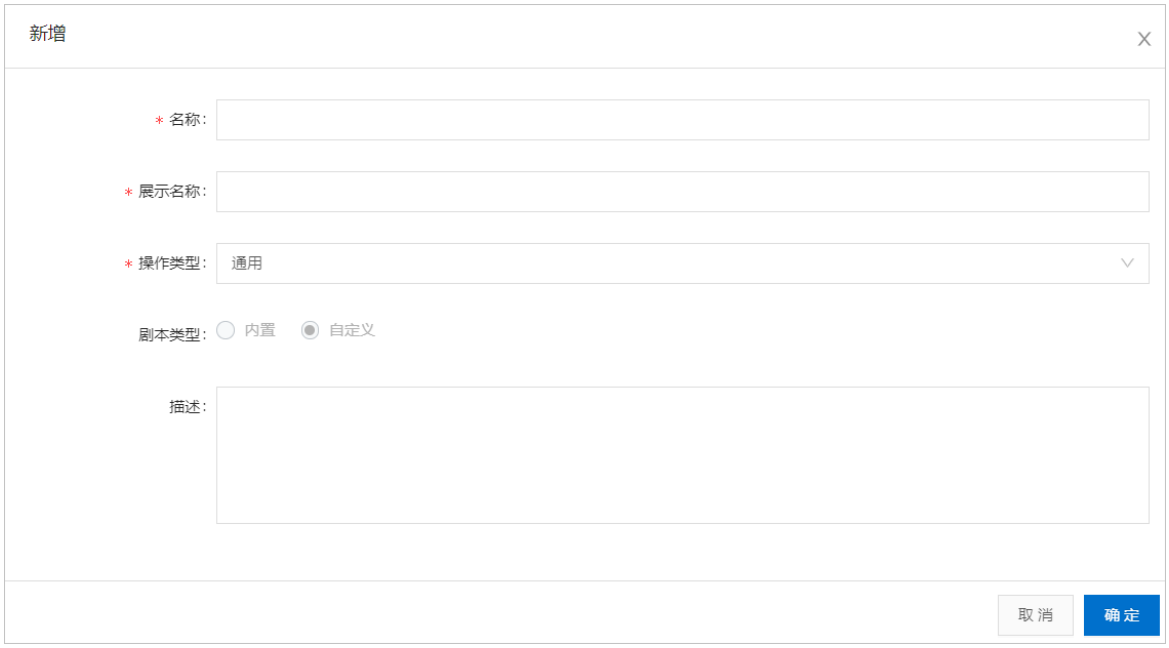
剧本列表展示剧本的基础信息、剧本状态以及运行记录。

- **名称**：自动化编排剧本的**名称**、**展示名称**。**名称**是剧本的唯一的名称标识，**展示名称**的设置利于使用者的可读性。
- **类型**：自动化编排剧本使用的模板，有**内置**和**自定义**两种类型。
- **执行计划**：执行剧本的时间。当剧本**执行方式**设置为**定时触发**时，可以设置执行一个剧本任务的周期：每天、每周、每月、每时、每分的对应某一时间点会启动剧本。
- **成功执行次数**：剧本执行成功的次数。如果一个告警触发了一个剧本，剧本顺利执行完成最后输出结果，则表示执行成功。
- **失败执行次数**：剧本执行失败的次数。
- **最新执行时间**：剧本最近一次执行的时间。
- **状态**：剧本目前所处的状态，有**已启用**和**已禁用**两种状态。

管理剧本

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>自动化编排>剧本列表**。

5. 在**剧本列表**页面右上角，单击**新增**。
6. 在**新增**对话框，配置剧本信息。



配置项	说明
名称	自动化编排流程的名称。
展示名称	自动化编排流程的展示名称。
操作类型	自动化编排流程的操作类型，可选值：**通用**、**调查**、**止血**、**缓解**。
剧本类型	自动化编排剧本使用的模板，有**内置**和**自定义**两种类型。
描述	自动化编排剧本的介绍。

7. 单击**确定**，提示**新建完成**。
8. （可选）在自动化编排流程编辑页面，绘制自动化编排流程图。

   完成新建剧本后，自动跳转到自动化编排流程编辑页面，单击剧本列表名称列的剧本名称，也可进入自动化编排流程编辑页面。

   > 注意 **剧本类型**选择**自定义**的剧本需要手动绘制流程图。

   i. 在剧本列表中，单击剧本名称。
   ii. 在**编辑**页面，将左侧导航栏中的组件与基础节点拖拽到可视化流程编辑画布中，按照业务流程绘制流程图。
   iii. 选中流程图中各组件，在**编辑**页面右侧的**基本信息**页面，查看和配置组件基本信息。

iv. 选中流程图中各组件，单击组件右侧的 图标，调试流程图。

您也可单击画布左上方的**断点调试**，以调试模式执行。

在画布下方的**历史执行记录**页签，您可以查看执行结果。



v. 单击画布左上方的**保存并发布**，系统会保存并启用自动化编译流程。

vi. 单击右上角**返回**。

发布成功后，剧本列表中剧本**状态**为**已启用**。

如单击画布左上方的**保存**时，系统只保存、暂不启用流程。剧本列表中剧本**状态**为**已禁用**。

在**剧本列表**的操作列对剧本可执行以下操作：

> 注意 只能对**已启用**的剧本执行**运行情况**、**设置**和**删除**操作。

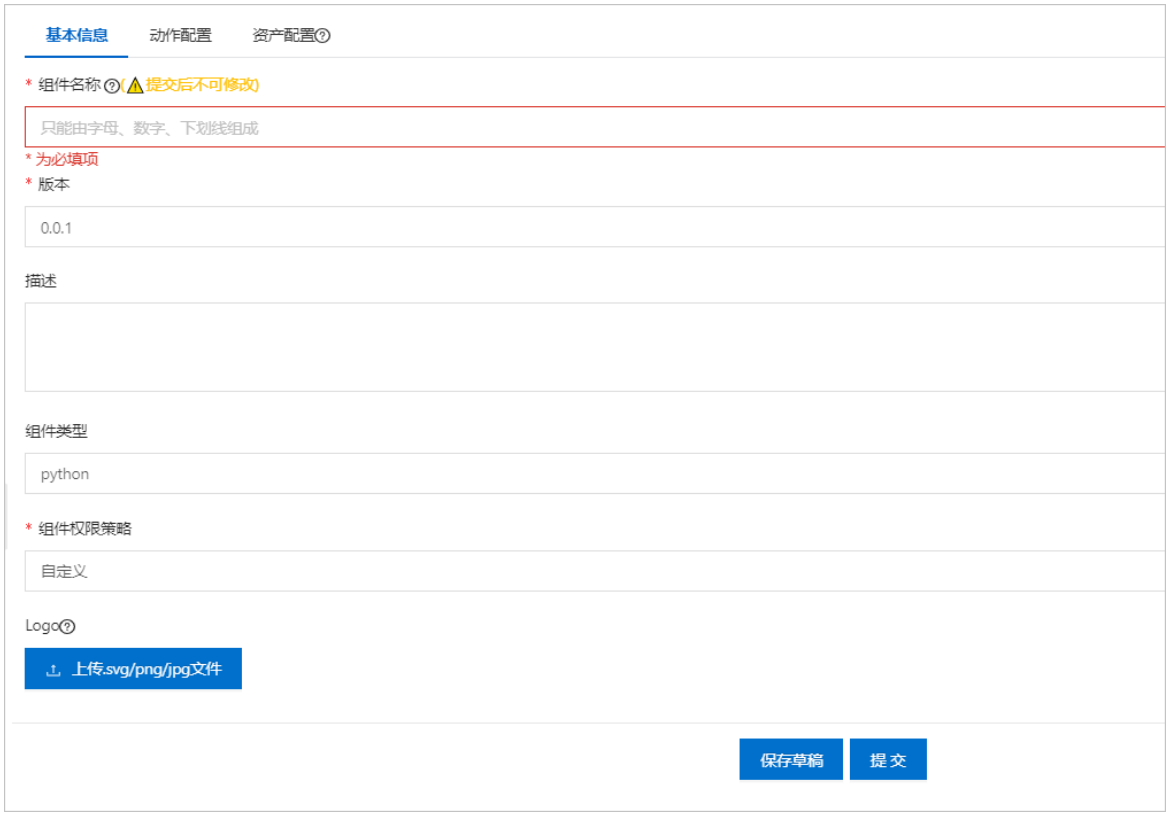
- 查看运行情况：单击**运行情况**，在**剧本执行日志**页签和**执行动作**页签，可以查看剧本的运行情况。
- 更新流程参数：单击**设置**，在**编辑**对话框修改自动化编排流程信息，单击**确定**。

  名称及**剧本类型**不能修改。
- 复制剧本：如需要新增的剧本与已有剧本配置相似，可以在已有剧本**操作**列，单击**复制**。在**复制**对话框，配置新剧本的**名称**、**展示名称**和**描述**，单击**确定**。
- 删除剧本：在需删除剧本的**操作**列，单击**删除**。在**确认删除吗？**对话框，单击**确定**。

10.11.2.2. 组件列表管理

组件是一个或几个完成特定事项资产、动作的集合。当需要跟外部服务连接时，组件可以是一个外部服务的管理器，例如WAF、防火墙、数据库或通知服务等。本文介绍如何新增、查看、编辑组件及组件中的资产、动作。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>自动化编排>组件列表**。
5. 在**组件列表**页面，单击右上角的**新增**。
6. 在**新增**页面的**基本信息**页签，配置组件的基本信息。



参数	说明
组件名称	自动化编排流程中组件的名称。 名称必须唯一，由字母、数字、下划线（_）组成，提交后不可修改。
版本	组件的版本号。
描述	组件的详细介绍。
组件类型	组件类型支持Java组件和Python组件两种。 Python组件中用到的第三方Python库没有安装且需要安装第三方Python包时，可在**云安全管理中心（SOC） > 响应编排 > 系统配置 > 第三方包管理**中安装。
组件权限策略	组件的权限策略，可选值：**内置**、**自定义**。 系统自带的组件为内置组件，新增的组件请选择**自定义**。自定义组件在**组件列表**页面，可以做修改操作，例如支持上传组件的代码zip包。内置组件在**组件列表**页面，不支持修改。
Logo	组件显示的图标素材，支持SVG、PNG、JPG格式的图片，建议使用SVG格式图片。 素材可以从阿里Icon Font网站下载。

7. 在**动作配置**页签，单击**添加动作**，配置组件的动作信息。

i. 配置动作基本信息。



参数	说明
名称	组件动作的名称。
操作类型	组件动作业务类型的分类，可选值：**通用**、**调查**、**止血**、**缓解**。
危险等级	动作操作的危险等级，可选值：**低**、**中**、**高**。
容量定义	动作执行的最大容量定义。 单击**容量定义**，在**容量定义**对话框，设置动作执行的最大容量，单击**确定**。
描述	组件动作的介绍。
自定义模板	该组件的配置面板是否需要通过上传JS文件来实现。开启**自定义模板**时，开关状态为，表示需要上传JS文件。 通常根据动作定义的输入参数的**交互方式**能否满足需求，来决定是否需要上传JS文件。当开启**自定义模板**开关时，**组件列表**页面会显示JS图标，可上传前端JS文件。

ii. 在**配置输入参数**区域，单击**新增**，配置动作的输入参数。



参数	说明
名称	动作输入参数的名称。
类型	参数类型，可选 值：**String**、**Long**、**Int**、**Double**、**DateTime**、**Boolean**、**Text**、**Complex**、**Summary_Raw**、**实体**。
描述	参数的介绍。
交互方式	资产配置时Form表单的交互方式。 单击下拉框，在**交互方式**对话框，选择**表单类型**。**表单类型**可选值有：**输入框**、**选择框**、**编辑器**。根据界面提示信息配置表单参数，单击**确定**。
必填	该参数是否为必填项，选中该项则表示参数是必填项。
默认值	设置参数默认值。

iii. 在**配置输出参数**区域，单击**新增**，配置动作的输出参数。



参数	说明
名称	动作输出参数的名称。
类型	参数类型，可选 值：**String**、**Long**、**Int**、**Double**、**DateTime**、**Boolean**、**Text**、**Complex**、**Summary_Raw**、**实体**。

8. （可选）在**资产配置**页签，单击**新增**，配置参数字段。

当组件执行动作需要用到必须且固定的信息时，可以将这些信息字段定义为组件资产。例如，账号密码等访问凭证信息、数据库连接信息等。



参数	说明
名称	资产的参数名称。
类型	参数类型，可选值：**String**、**Long**、**Int**、**Double**、**DateTime**、**Boolean**、**Text**、**Complex**、**Summary_Raw**、**实体**。
描述	参数的介绍。
交互方式	资产配置时Form表单的交互方式。 单击下拉框，在**交互方式**对话框，选择**表单类型**。**表单类型**可选值为：**输入框**、**选择框**、**编辑器**。根据界面提示信息，配置表单参数，单击**确定**。
必填	该参数是否为必填项，选中该项则表示参数是必填项。
加密	**类型**为密码类型参数时需要设置，选中该项表示参数需要加密。
默认值	设置参数默认值。

9. 在**新增**页面，单击**提交**。根据界面提示，将zip包保存到本地。

   界面提示保存的zip包为自定义组件的代码模板，上传组件的代码zip包时可作为代码模板使用。

   > **说明** 单击**保存草稿**时，配置的信息会缓存到本地，在**组件列表**页面不显示配置的组件。

   提交成功后，在**组件列表**页面，可以查看组件及其动作、资产信息：

   - 编辑资产：单击组件名后的图标，在**资产列表**页面，可新增、编辑、删除资产。
   - 编辑组件：单击组件名后的 图标，在**编辑**页面，可以修改组件基本信息、资产信息、动作信息，单击**提交**。
   - 上传组件的代码zip包：创建组件时**组件权限策略**选择**自定义**的组件，可以上传组件的代码zip包。打开保存到本地的代码模板zip包，如为Python类型组件需打开*main.py*文件，在和动作同名的函数中，增加您需要的逻辑支持代码。例如：

```
#coding=utf-8
from utils.Result import Result
import requests
import json
#coding=utf-8
def sendRequest(headers,post_data,method,url):
    if(method=='get'):
        r = requests.get(url,params={})
        resultBody = json.loads(r.text)
        data = []
        data.append({"respBody": resultBody,"status":r.status_code})
    #print data    result = Result(actionRes, data)
    #dataArray一般用于动作中会获取数据输出到自动化编排流程下一结点的情况    #example
    return result
if __name__ == '__main__':
    sendRequest("","","get","http://11.158.114.96/sao/getallactives")
```

在代码输出的data中返回该组件的执行结果，在上面例子中返回了status和respBody， 在流程中可以使用 `<nodeName>.datalist.*.status` 和 `.datalist.*.respBody` 来读取这些值。

修改之后，把代码打包成zip文件，名字改为组件名称一样。

在**组件列表**页面，单击组件名后的图标，上传组件的代码zip包。

- 上传前端JS文件：当组件的动作输入参数，开启**自定义模板**开关时，**组件列表**页面会显示图标，可上传前端JS文件。
- 在线编辑资产、动作参数：单击组件后的 图标，单击**编辑器**页面的**设置参数**，可以设置动作参数、添加资产。
- 删除组件：单击组件名后的图标，在对话框中单击**确定**，从组件列表中删除组件。
- 查看资产、动作参数信息：在资产或动作区域单击>图标，在展开的资产或动作列表，单击资产或动作前面的+图标，可以查看资产或动作的参数信息。

10.11.3. 知识管理

10.11.3.1. 情报管理

情报管理实现对恶意指标的管理，展示所有封禁的威胁指标IOC（Indicator Of Compromise），可以查看、封禁、解封恶意指标。本文介绍了如何查看情报总览信息和如何新增、删除、查看情报详情。

查看情报统计信息

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>知识管理>情报管理**。
5. 在**情报管理**页面，查看情报统计情况。



情报管理页面区域说明表

区域	说明
总情报数量	当前阿里云账号的情报总数。
已封禁情报数量	当前阿里云账号统计周期内封禁的情报的数量。并进一步细分为，临时封禁数量和永久封禁数量。支持今日和本周统计周期： ○ 今日数据显示当日00:00起到当前时间新增的情报数（总数=临时数+永久数）。 ○ 本周数据显示自然周周日00:00到当前时间新增的情报（总数=临时数+永久数）。
已解封情报数	当前阿里云账号统计周期内解封的情报的数量。支持今日和本周统计周期： ○ 今日数据显示当日00:00起到当前时间解封的情报数。 ○ 本周数据显示自然周周日00:00到当前时间解封的情报。
已隔离主机数量	当前阿里云账号统计周期内已经隔离的主机数量。支持今日和本周统计周期： ○ 今日数据显示当日00:00起到当前时间隔离的主机总数。 ○ 本周数据显示自然周周日00:00到当前时间隔离的主机总数。

查看情报列表

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>知识管理>情报管理**。
5. 在**情报管理**页面，查看情报列表。



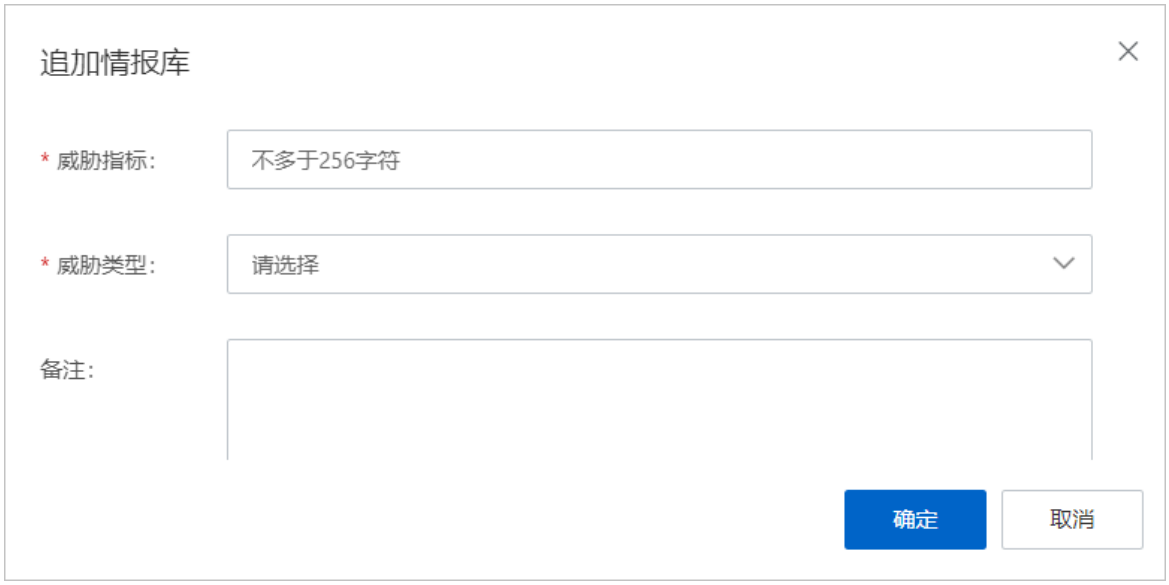
威胁指标	威胁类型	封禁类型	首次封禁时间	解封时间	操作
[redacted]	IP	--	--	--	详情 | 追加情报库 | 移除情报库
[redacted]	IP	NDR	2021-12-09 14:11:59	23 天	详情 | 追加情报库 | 移除情报库
[redacted]	IP	--	--	--	详情 | 追加情报库 | 移除情报库
[redacted]	IP	--	--	--	详情 | 追加情报库 | 移除情报库
[redacted]	IP	NDR	2021-12-08 11:43:14	22 天	详情 | 追加情报库 | 移除情报库

情报列表展示参数说明表

参数	说明
威胁指标	IP、文件hash等指标内容。添加后不允许修改。
威胁类型	威胁指标的类型，可选值：**主机名**、**应用名**、**数据库**、**文件hash**、**AccesskeyID**、**文件MD5**、**服务器IP**、**域名**、**cna**、**Aegis文件**。
封禁类型	通过SOAR下发的封禁策略，可能有多个：**NDR**、**WAF**。不含用户手动在WAF、NDR内配置的封禁规则。
首次封禁时间	通过SOAR首次封禁该威胁的时间。
解封时间	解封时间到当前系统时间的长度，单位天。

管理情报详情

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>知识管理>情报管理**。
5. 在**情报管理**页面，单击**新建**。
6. 在**追加情报库**对话框，配置情报的基本信息。



参数	说明
威胁指标	威胁指标的内容。 由1~256字符组成，且支持特殊字符。
威胁类型	威胁指标的类型，可选值：**主机名**、**应用名**、**数据库**、**文件hash**、**AccesskeyID**、**文件MD5**、**服务器IP**、**域名**、**cna**、**Aegis文件**。
（可选）**备注**	威胁情报添加的备注信息。 不超过200字符，支持中文、英文、数字。

7. 单击**确认**。

   在配置情报信息参数后，在**情报管理**页面，可以查看情报信息。

   - 查询情报：支持通过输入威胁指标进行查询，还支持设置起始日期和结束日期时间段，对安全事件的创建时间进行过滤。
   - 删除情报：选中需要删除的情报前的复选框，单击情报列表左上方的删除，即可在情报列表中删除选定情报。
   - 查看情报参数信息：在情报列表中，单击威胁指标的后的**详情**。在**详情**页面，可以查看和添加**封禁记录**。添加**封禁记录**的操作如下：
     a. 在**封禁记录**页签，单击**添加**。
     b. 在**人工封禁**对话框，配置具体参数。

参数	说明
封禁类型	通过SOAR下发的封禁策略，可选值：**NDR封禁**、**WAF封禁**。
规则名称	为此条封禁设置的规则名称。
源IP地址	设置威胁指标的源IP地址。
（可选）**目的IP地址**	设置威胁指标的源目的IP地址。
（可选）**目的端口**	设置威胁指标的目的端口。
封禁时间	当前系统时间到解封时间的长度，可选值：**一天**、**一周**、**一个月**、**永久**。
组织	选择封禁的组织名称。
防护站点id	输入防护站点id.

     c. 单击**确定**。

10.11.3.2. 名单库

名单库用于记录安全事件处理过程中积累的各种数据，用于积累处理经验和数据的重复利用。名单库有**知识库**和**维表**两种类型。本文介绍了如何创建名单库和查看名单库信息。

创建名单库

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>知识管理>知识库**。
5. 在知识库页面，单击**新增名单库**。
6. 在**新增名单库**对话框，设置名单库参数。



新增名单库参数说明表

参数	说明
名单库名称	设置名单库的名称。
名单库ID	设置名单库的ID。
名单库类型	在下拉框中选择名单库的类型，可选值有：**知识库**、**维表**。知识库的每条知识记录一个维度的内容，维表的每条知识内容可以记录两个属性的内容。
描述	设置名单库的描述信息。

新增的名单库显示在名单库列表中。

7. 选择**新增名单库**，单击页面右上方**新增**。
8. 在**新增名单**对话框，设置名单参数。

名单库有**知识库**和**维表**两种类型，不同类型的名单库需要设置的参数不同。

- 选择**名单库类型**为**知识库**时：



参数	说明
内容	名单内容。可以是IP地址、文本、字符串、数字等内容。内容最大不超过200字符，支持中文、英文、特殊字符 `@#¥%&*（）——+` 。
描述	名单的描述信息。
过期时间	名单内容的有效期，超出有效期的内容自动删除。可选值有：**永久有效**、**7天**、**90天**、**180天**、自定义。默认为**永久有效**。

- 选择**名单库类型**为**维表**时：



参数	说明
Key	一个属性的名单内容。可以是IP地址、文本、字符串、数字等内容。内容最大不超过200字符，支持中文、英文、特殊字符 `@#¥%&* () —+` 。
Value	另一个属性的名单内容。可以是IP地址、文本、字符串、数字等内容。内容最大不超过200字符，支持中文、英文、特殊字符 `@#¥%&* () —+` 。
描述	名单的描述信息。
过期时间	名单内容的有效期，超出有效期的内容自动删除。可选值有：**永久有效**、**7天**、**90天**、**180天**、自定义。默认为**永久有效**。

9. 单击**确认**。
   创建的名单库会显示在**知识库**页面左侧的名单库列表中，创建的名单会显示在名单库列表的名单列表中。

查看名单库信息

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在**选择访问**卡片，选择**地域**，单击**角色访问授权**。
4. 在左侧导航栏，选择**响应编排>知识管理>知识库**。
5. 在**知识库**页面，在文本框输入名单库的**创建人**、**名称**、**类型**或**名单ID**，单击搜索图标。



6. 在名单库列表，查看指定名单库的**创建人**、**名单库名称**、**名单库ID**。

   在名单库列表页面，您还可以进行以下操作：

   - 编辑名单库：在名单库列表**操作**列，单击 ，您可以在**编辑名单库**对话框，修改**名单库名称**、**描述**。
   - 删除名单库：在名单库列表**操作**列，单击 ，在**确认删除吗？**对话框单击**确认**，可以删除所在行的名单库。

7. 在指定名单库右侧，查看名单详细信息。

   名单库有**知识库**和**维表**两种类型，不同类型的名单库显示的信息不同。

   - 选择**名单库类型**为**知识库**时：



参数	说明
内容	名单内容。可以是IP地址、文本、字符串、数字等内容。内容最大不超过200字符，支持中文、英文、特殊字符 `@#¥%&*（）——+` 。
描述	名单的描述信息。
创建者	名单的添加者。
最后修改	此条名单的最后修改时间。
过期时间	名单内容的有效期，超出有效期的内容自动删除。
操作	能对名单进行的操作。

- 选择**名单库类型**为**维表**时：



参数	说明
Key	名单一个属性的内容。可以是IP地址、文本、字符串、数字等内容。内容最大不超过200字符，支持中文、英文、特殊字符 `@#¥%&*（）——+` 。
Value	名单另一个属性的内容。可以是IP地址、文本、字符串、数字等内容。内容最大不超过200字符，支持中文、英文、特殊字符 `@#¥%&*（）——+` 。
描述	名单的描述信息。
创建者	名单的添加者。
最后修改	名单的最后修改时间。
过期时间	名单内容的有效期，超出有效期的内容自动删除。可选值有：**永久有效**、**7天**、**90天**、**180天**、**自定义**。默认为**永久有效**。
操作	能对名单进行的操作。

在名单列表页面，您还可以进行以下操作：

- 编辑名单：在名单列表**操作**列，单击**编辑**，您可以在**编辑名单**对话框，修改**Key**、**Value**、**描述**、**过期时间**。
- 删除名单：在名单列表**操作**列，单击**删除**，在**确认删除吗？**对话框单击**确认**，可以删除所在行的名单。
- 启用、禁用名单：在名单列表**操作**列，打开**启用**开关，则可启用名单。关闭**启用**开关，则禁用名单。

10.11.4. 系统配置

10.11.4.1. 环境变量配置

本文介绍了如何配置环境变量。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**响应编排**。

4. 在**响应编排**页面左侧导航栏，选择**系统配置 > 环境变量配置**。
5. 在**环境变量配置**页面上方的搜索框，输入环境变量配置的Key/Value/描述。
6. 单击搜索图标。在环境变量配置列表，查看环境变量配置信息。

   在环境变量配置列表，您还可以进行以下操作：

   - 编辑环境变量配置：在环境变量配置列表**操作**列，单击**编辑**，您可以在**编辑名单**对话框，修改**Key**、**Value**、**描述**、**过期时间**。



参数	说明
Key	一个属性的环境变量配置内容。环境变量中的key为系统后台的基础参数设置，包括系统所属的region、租户、AK等。不建议随便增加。只需要每个局点根据实际情况更新对应Key的Value。
Value	另一个属性的环境变量配置内容。环境变量中的key为系统后台的基础参数设置，包括系统所属的region、租户、AK等。不建议随便增加。只需要每个局点根据实际情况更新对应Key的Value。
描述	环境变量配置的描述信息。

参数	说明
过期时间	环境变量配置内容的有效期。可选值有：**永久有效**、**7天**、**90天**、**180天**、自定义。默认为**永久有效**。

- 删除环境变量配置：在环境变量配置列表**操作**列，单击**删除**，在**确认删除吗？**对话框单击**确定**，可以删除所在行的环境变量配置。
- 启用、禁用环境变量配置：在环境变量配置列表**操作**列，打开 启用 开关，则可启用环境变量配置。关闭**启用**开关，则禁用环境变量配置。
- 新增环境变量配置：单击**环境变量配置**页面的**新增**，输入信息参数。

10.11.4.2. 管理流式数据源

本文介绍如何新增、搜索、删除、编辑流式数据源。

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**响应编排**。
4. 在**响应编排**页面左侧导航栏，选择**系统配置 > 流式数据源**。
5. 在**流式数据源**页面，单击**新增**。
6. 在**新增**对话框，配置流式数据源参数。
7. 单击**确认**。
   新增的数据源显示以在流式数据源列表中。
8. 在流式数据源列表，查看流式数据源的**名称**、**类型**、首次创建时间、最后修改时间和**状态**。



在流式数据源列表，您还可以进行以下操作：

- 搜索流式数据源：在流式数据源列表上方的搜索框，输入流式数据源的名称、类型、创建人。
- 删除流式数据源：在流式数据源列表**操作**列，单击**删除**，在**确认删除吗？**对话框单击**确定**，可以删除所在行的流式数据源。
- 编辑流式数据源：在流式数据源列表**名称**列，单击需要修改的流式数据源名称，在**编辑**对话框，修改流式数据源信息。

10.11.4.3. 管理第三方包

Python类型组件中用到的第三方Python库支持安装第三方Python包。本文介绍如何查看和安装第三方包。

操作步骤

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**响应编排**。
4. 在**响应编排**页面左侧导航栏，选择**系统配置 > 第三方包管理**。
5. 在**第三方包管理**页面，选择安装方式并配置安装包信息，单击**安装**。

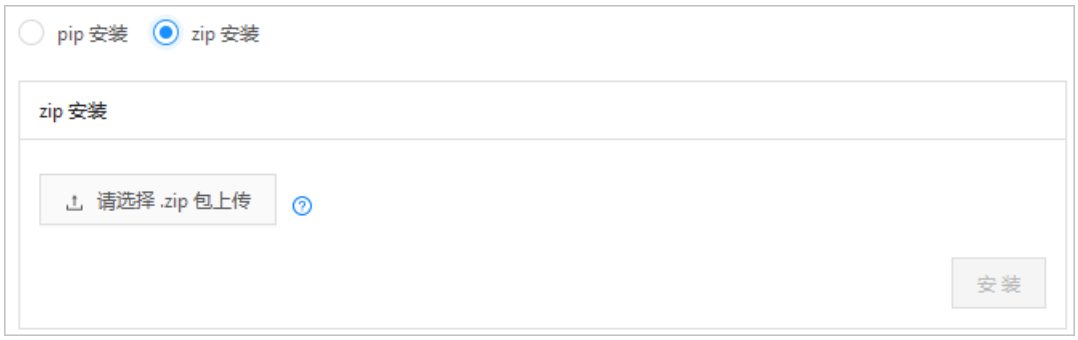
   Python类型组件支持两种方式安装第三方包：

   - **pip安装**：当系统可以访问因特网时，可以选择**pip安装**方式。

     在**pip安装**区域输入**包名**，系统会从官方站点下载对应的第三方Python包。

   - **zip安装**：当系统不能访问因特网时，可以选择**zip安装**方式。

     将*.whl*格式的安装包压缩为*.zip*格式，单击 请选择 .zip 包上传按钮上传安装包。

执行结果

安装成功后，在**安装记录**列表可以查看已经安装成功的第三方包**包名称**、**版本**等信息。



10.11.4.4. 剧本执行日志

本文介绍如何查看剧本执行日志。

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云安全管理中心SOC**。
3. 在左侧导航栏，单击**响应编排**。
4. 在**响应编排**页面左侧导航栏，选择**系统配置 > 剧本执行日志**。
5. 单击**剧本执行日志**页签或**执行动作**页签。
   - 单击**剧本执行日志**页签，查看剧本执行日志信息。
     a. 在**剧本执行日志**页签的搜索框，输入搜索参数。
     b. 单击搜索图标。
     c. 在剧本执行日志列表，查看剧本执行日志信息。

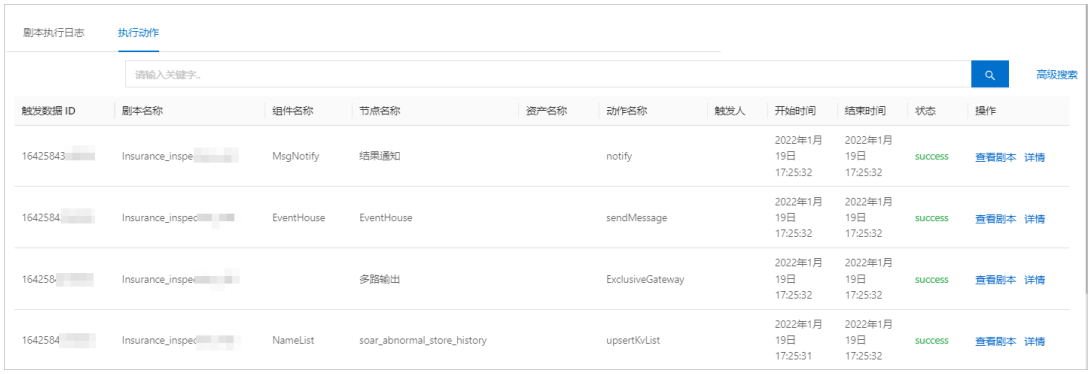


在剧本执行日志列表，您还可以进行以下操作：

- 执行动作：单击剧本执行日志列表**操作**列的**执行动作**，进入**执行动作**页面，可以查看执行动作的**完整输出结果**、**输入参数**、**输出参数**、**运行日志**。
- 查看数据源：单击剧本执行日志列表**操作**列的**查看数据源**，您可以查看数据源。
- 查看剧本：单击剧本执行日志列表**操作**列的**查看剧本**，跳转到剧本列表页面，您可以查看剧本信息。
- 重放剧本：单击剧本执行日志列表**操作**列的**重放**，在**输入参数**对话框单击**确定**即可使用相同的数据源，重新执行剧本。

   - 单击**执行动作**页签，查看执行动作信息。
     a. 在**执行动作**页签的搜索框，输入搜索参数。
     b. 单击搜索图标。

c. 在执行动作列表，查看执行动作信息。



在剧本执行动作列表，您还可以进行以下操作：

- 查看剧本：单击剧本执行动作列表**操作**列的**查看剧本**，跳转到剧本列表页面，您可以查看剧本信息。
- 查看运行详情：单击剧本执行动作列表**操作**列的**详情**，您可以查看运行详情信息。

10.12. 容器防护

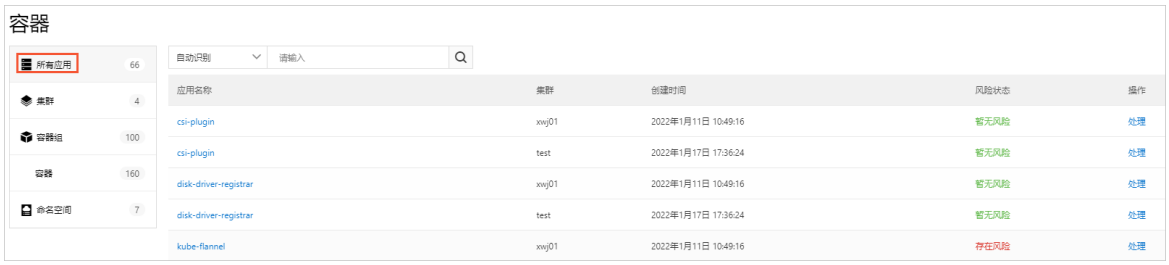
10.12.1. 查看容器服务ACK应用

本文介绍了如何查看容器服务ACK应用的详细信息。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**主机安全 > 容器防护**。
3. 在**容器防护**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**容器防护 > 资产中心 > 容器**。
5. 在**容器**页面，单击**所有应用**。

   容器列表分页展示了应用的**应用名称**、**集群**、**创建时间**和**风险状态**。



6. 单击应用名称或**操作**列**处理**。

   您可以查看应用的**漏洞风险**、**告警风险**、**容器组**。同时，您可以查看风险的详情及对其进行处理。

10.12.2. 查看ACR镜像

本文介绍了如何查看ACR镜像。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**主机安全 > 容器防护**。
3. 在**容器防护**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**容器防护 > 资产中心 > 镜像**。
5. 在**镜像**页面，单击**镜像**或**存在风险的镜像**。

   镜像列表分页展示了镜像的**镜像地址/标签**、**镜像大小**、**最新发现时间**和**风险状态**。



6. 定位到有风险的镜像，单击**操作**列**处理**。

   您可以查看镜像的**镜像系统漏洞**、**镜像应用漏洞**、**镜像基线检查**和**镜像恶意样本**的基本信息。同时，您可单击**操作**列**详情**，查看对应的详细信息。

10.12.3. 镜像安全扫描

容器防护ACK支持对ACR镜像仓进行安全扫描，包括扫描镜像漏洞、基线问题、恶意样本等。

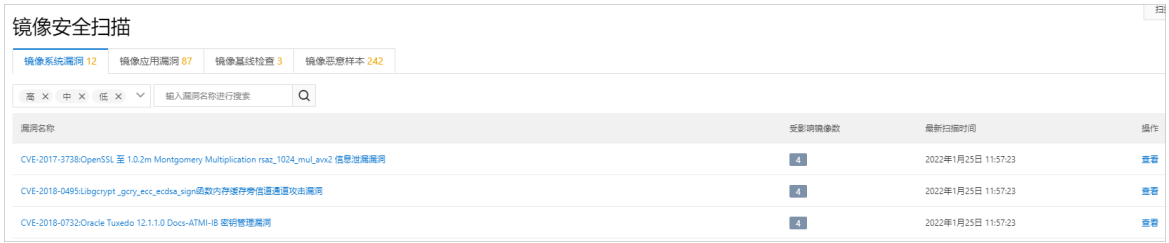
背景信息

镜像安全扫描功能支持对镜像中存在的高危系统漏洞、应用漏洞、恶意样本、配置风险和敏感数据进行检测和识别。镜像上的基础系统软件、中间件、Web应用、数据库服务等，可能会存在挖矿木马、后门程序等安全漏洞，基于风险镜像运行的容器回危害您的资产安全。执行镜像安全扫描可以帮助您检测漏洞资产中是否存在镜像漏洞和恶意样本，并提供漏洞修复方案，为您提供一站式漏洞管理能力，让镜像漏洞修复更简单。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**主机安全 > 容器防护**。
3. 在**容器防护**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**容器防护 > CI/CD安全 > 镜像安全扫描**。
5. 在**镜像系统漏洞**或**镜像应用漏洞**页签，单击**漏洞名称**或**操作**列**查看**。

   您可以查看漏洞详情和受影响的镜像详情。



6. 在**镜像基线检查**页签，单击**操作**列**详情**。

   您可查看对应基线**镜像地址/版本**和**检查详情/总检查项**。您还可以单击**操作**列**详情**，查看风险项的状

态并对其进行**加白名单**或**取消加白**操作。



7. 在**镜像恶意样本**页签，单击**恶意样本**名称或**操作**列**详情**。

   您可以查看对应的恶意样本详情和受影响的镜像详情。



10.12.4. 入侵事件告警

容器防护ACK支持检测ACK集群节点、容器，可提供病毒木马、外部入侵、供应链攻击、越权逃逸等维度的风险监控拦截能力。

背景信息

入侵事件告警功能是基于阿里云大数据告警模型，安骑士威胁检测模块具备丰富的入侵检测能力，能够帮助用户掌握ACK环境威胁情况，有效拦截外部风险。

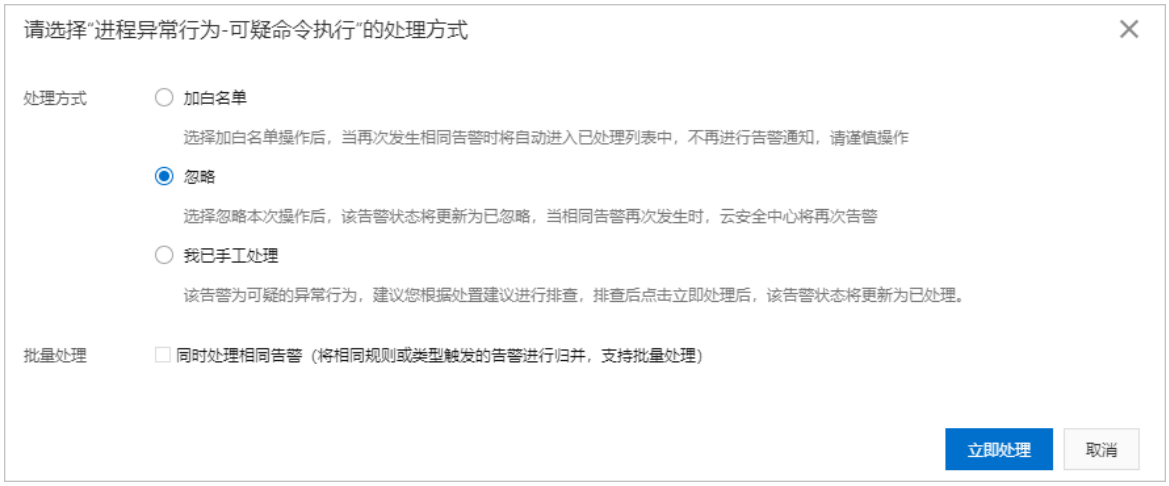
操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**主机安全 > 容器防护**。
3. 在**容器防护**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**容器防护 > 运行时防护 > 入侵事件告警**。
5. 在**入侵事件告警**页面，单击**受影响资产**的名称。

   您可以查看容器的详情。 同时，您也可以将光标放置在**受影响资产**名称上，您可查看该资产的详细信息。

6. 在**入侵事件告警**页面，单击**操作**列**处理**。

   您可以对该入侵事件进行**加白名单**、**忽略**、**我已手工处理**和**批量处理**等操作。



7. 在**入侵事件告警**页面，单击告警名称或**操作**列**详情**。

   您可以查看该入侵事件的具体信息。

10.12.5. 日志检索

日志检索功能提供ACK容器的进程快照、网络连接、进程启动的日志查询，支持前缀模糊匹配查询。

背景信息

入侵事件告警功能是基于阿里云大数据告警模型，安骑士威胁检测模块具备丰富的入侵检测能力，能够帮助用户掌握ACK环境威胁情况，有效拦截外部风险。

操作步骤

1. 登录云盾安全中心。
2. 在顶部菜单栏，将光标放置在**安全**上，选择**主机安全 > 容器服务**。
3. 在**容器服务**授权页面，选择**地域**并单击**角色授权访问**。
4. 在左侧导航栏，选择**容器防护 > 日志检索**。
5. 在**日志检索**页面，选择**日志源**、**日志字段**、**查询条件**、**关键字**，单击**搜索**。

   您可以选择的查询时间包括**24小时内**、**7天内**，同时您还可以**自定义时间**。**自定义时间**不能超过30个自然日。

11.云盾系统配置

11.1. 规则运营

11.1.1. 添加流量安全监控IPS规则

本文介绍如何添加云防火墙的流量安全监控IPS规则。云防火墙已经内置IPS规则，如果您需要根据自身的业务需求和网络环境自定义IPS规则，可以参考本文设置。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，选择**全局平台安全 > 云盾**。
3. 在左侧导航栏，单击**规则运营**。
4. 单击**云防火墙IPS规则运营**页签。
5. 单击**添加自定义规则**。
6. 在**添加自定义规则**页面，设置规则参数。

参数	说明
规则名称	设置自定义IPS规则的名称，建议使用可识别规则用途的名称，便于后续管理。
规则引擎	在下拉栏中选择规则引擎，可选**基础规则**和**虚拟补丁**。
攻击类型	在下拉栏中选择该规则的攻击类型。
等级	在下拉栏中选择威胁等级，可选**低危**、**中危**和**高危**。
CVE	设置该规则的CVE编号。 **说明** 通用漏洞披露CVE（Common Vulnerabilities and Exposures）列出了已公开披露的各种计算机安全缺陷。CVE编号由CVE编号管理机构（CNA）分配。
攻击应用	设置攻击应用名称。
规则模式	在下拉栏中选择IPS检测的规则模式，可选**包模式**和**流模式**。
方向	在下拉栏中选择IPS检测的流量方向，可选**双向**、**入向**和**出向**。
规则内容	设置规则内容，规则采用Snort语法。 **说明** 添加规则内容时请确认正确性，不正确的规则内容可能会影响您的业务。
规则描述	设置规则描述信息，建议使用规则用途、影响等信息，便于后续管理。

参数	说明
备注	设置规则备注信息，建议使用规则用途、影响等信息，便于后续管理。

7. 单击**确定**，完成添加自定义IPS规则操作。

11.1.2. 管理云防火墙IPS规则

本文介绍如何查看、启用和禁用云防火墙的IPS规则。

背景信息

在**云防火墙IPS规则运营**中，您可以查看云防火墙的IPS规则（包括内置规则和自定义规则），并根据业务需要启用或禁用规则。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**规则运营**。
4. 单击**云防火墙IPS规则运营**页签。
5. 管理云防火墙IPS规则。

   在IPS规则列表中，您可以查看规则详情、启用规则和禁用规则。

   - 查看规则详情

     定位到某一规则，单击**操作**列中的**详情**，您可以查看该规则的具体信息。

   - 启用规则

     如果需要启用某个规则，则定位到该规则，单击**启用状态**列中的切换开关，将**禁用**切换为**启用**。

   - 禁用规则

     如果某个规则不适应于您的业务环境，您可以禁用该规则。

     定位到该规则，单击**启用状态**列中的切换开关，将**启用**切换为**禁用**。

11.1.3. 添加流量安全监控IDS规则

本文介绍如何添加流量安全监控IDS规则。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**规则运营**。
4. 在规则运营页面，单击**流量安全监控IDS规则运营**页签。
5. 单击**添加自定义规则**。
6. 在**添加自定义规则**面板，设置规则参数。

参数	说明
规则名称	设置自定义IPS规则的名称，建议使用可识别规则用途的名称，便于后续管理。
规则引擎	在下拉栏中选择规则引擎，可选**基础规则**和**虚拟补丁**。
攻击类型	在下拉栏中选择该规则的攻击类型。
等级	在下拉栏中选择威胁等级，可选**低危**、**中危**和**高危**。
CVE	设置该规则的CVE编号。 **说明** 通用漏洞披露CVE（Common Vulnerabilities and Exposures）列出了已公开披露的各种计算机安全缺陷。CVE编号由CVE编号管理机构（CNA）分配。
攻击应用	设置攻击应用名称。
规则模式	在下拉栏中选择IPS检测的规则模式，可选**包模式**和**流模式**。
方向	在下拉栏中选择IPS检测的流量方向，可选**双向**、**入向**和**出向**。
规则内容	设置规则内容，规则采用Snort语法。 **说明** 添加规则内容时请确认正确性，不正确的规则内容可能会影响您的业务。
规则描述	设置规则描述信息，建议使用规则用途、影响等信息，便于后续管理。
备注	设置规则备注信息，建议使用规则用途、影响等信息，便于后续管理。

7. 单击**确定**，完成添加自定义流量安全监控IDS规则操作。

11.1.4. 管理流量安全监控IDS规则

本文介绍如何查看、启用和禁用流量安全监控IDS规则。

背景信息

在**管理流量安全监控IDS规则**中，您可以查看流量安全监控IDS规则（包括内置规则和自定义规则），并根据业务需要启用或禁用规则。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**规则运营**。
4. 单击**流量安全监控IDS规则运营**页签。
5. 管理流量安全监控IDS规则。

在流量安全监控IDS规则列表中，您可以查看规则详情、启用规则和禁用规则。

- 查看规则详情

  定位到某一规则，单击**操作**列中的**详情**，您可以查看该规则的具体信息。

- 启用规则

  如果需要启用某个规则，则定位到该规则，单击**启用状态**列中的切换开关，将**禁用**切换为**启用**。

- 禁用规则

  如果某个规则不适应于您的业务环境，您可以禁用该规则。

  定位到该规则，单击**启用状态**列中的切换开关，将**启用**切换为**禁用**。

11.1.5. 自定义DDoS清洗策略和牵引阈值

本文介绍如何自定义DDoS的清洗策略和牵引阈值。DDoS防护已经设置有默认的阈值，如果默认设置不符合您的网络环境，可以参考本文自定义阈值。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**规则运营**。
4. 自定义清洗策略的阈值。
   i. 单击**Aliguard规则运营**页签。
   ii. 在**Aliguard规则运营**也签下，单击**清洗策略**页签。
   iii. 在需要调整的规则的**操作**列，单击**调整阈值**。
   iv. 在**调整阈值**对话框中，输入阈值。
   v. 单击**确定**，完成调整阈值操作。
5. 自定义牵引阈值。
   i. 单击**Aliguard规则运营**页签。
   ii. 在**Aliguard规则运营**页签下，单击**牵引阈值**页签。
   iii. 在需要调整的策略的**操作**列，单击**调整阈值**。
   iv. 在**调整阈值**对话框中，输入阈值。
   v. 单击**确定**，完成调整阈值操作。

11.1.6. 查看安骑士规则

本文介绍如何查看安骑士规则的运营情况，可以查看漏洞列表、基线列表、主机异常列表。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**规则运营**。
4. 在**规则运营**页面，单击**安骑士规则运营**页签。

5. 在总览区域可以查看**漏洞库总数**、**基线**、**主机异常**、**引擎**。
6. 查看漏洞情况。
   i. 单击**漏洞**页签。
   ii. 在概览区域可以查看**Linux漏洞总数**、**Windows漏洞总数**、**Web-CMS漏洞总数**、**应急漏洞总数**。
   iii. 设置搜索项，查看漏洞列表。

   > **说明** 如果需要查看全部漏洞，可忽略此步骤。

   列表中可以查看**漏洞名称**、**CVE编号**、**漏洞类型**、**系统**、**更新时间**、**状态**。
7. 查看基线列表。
   i. 单击**基线**页签。
   ii. 在概览区域可以查看基线类型个数、基线检查项个数。
   iii. 设置搜索项，查看基线列表。

   > **说明** 如果需要查看全部基线，可忽略此步骤。

   列表中可以查看**基线类型**、**检查项类别**、**检查项名称**、**风险等级**、**更新时间**、**状态**。
8. 查看主机异常列表。
   i. 单击**主机异常**页签。
   ii. 在概览区域可以查看**规则告警子类型数**、Webshell和恶意病毒个数。
   iii. 设置搜索项，查看主机异常列表。

   > **说明** 如果需要查看全部异常情况，可忽略此步骤。

   列表中可以查看**子类名称**、**规则父类**、**风险等级**、**更新时间**、**来源**、**状态**。

11.2. 威胁情报

11.2.1. 查看总览

威胁情报总览页面展示近30天您资产中已遭受威胁的整体情况和统计数据。

前提条件

已开启**消费产品配置**功能，具体操作，请参见配置消费产品。

操作步骤

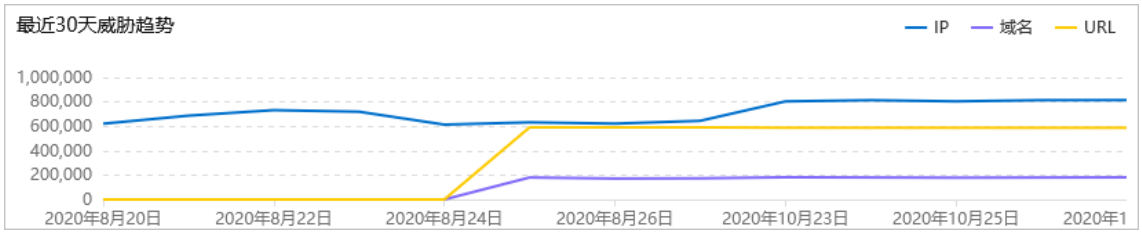
1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**总览**。
4. 在**总览**页面，查看威胁情报服务检测到的专有云已遭受的威胁事件和统计数据。
   您可以在**总览**页面执行以下操作：

- 查看**恶意指标情报总数**。

  在**总览**页面的**恶意指标情报总数**区域，查看检测到的专有云遭受的威胁情况，包括恶意IP总数、恶意域名总数、恶意URL总数。



- 查看**最近30天威胁趋势**。



- 搜索任意IP，确认其是否为恶意来源。

  在右上角的搜索框中输入您需要排查的IP，单击图标，跳转到**云安全管理中心（SOC） > 威胁情报 > IP搜索**页面显示**IP报告**查看报告详细信息，更多信息，请参见IP搜索。

- 查看**Top 10活跃IP恶意地址**。

  在**总览**页面的**Top 10活跃IP恶意地址**区域，查看排行Top 10的恶意IP列表，包括**IP地址**、**第一次恶意观察**、**最后的恶意观察**、**恶意标签**。定位到目标恶意IP地址，单击操作列的**查看**，跳转到**IP搜索**页面显示**IP报告**查看报告详细信息，更多信息，请参见IP搜索。

11.2.2. 查看IP搜索信息

威胁情报服务支持威胁情报搜索功能，可以搜索IP地址，帮助您及时有效排查存在风险的恶意IP。

前提条件

已开启**消费产品配置**功能，具体操作，请参见配置消费产品。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**IP搜索**。
4. 在**搜索**页面的搜索栏中，输入您需要查询的可疑或恶意IP地址，然后单击图标。
5. 在**IP报告**页面，查看该IP地址的**威胁等级**、**基本信息**、**威胁概述**、**IP详情**、**攻击风险程度分析**等信息。



报告信息如下所示：

- **威胁等级**：查看该可疑或恶意IP的威胁等级。

  威胁情报服务将IP地址划分为正常、可疑和高危3个威胁等级。如果检索的IP地址被识别为高危等级，建议您立即对该IP地址进行处理。

- **基本信息**：查看该可疑或恶意IP的基本信息。

  该IP地址的基本信息包括所在IDC服务器、ASN编码、国家、城市、域名关联数等信息。

- 查看该可疑或恶意IP的威胁统计数据。

  您可以在威胁统计模块查看该IP的**威胁概述**、**IP详情**和**威胁详情**。

  - **威胁概述**页签为您展示了该IP地址的**Top 5攻击偏好**、**攻击数量**、**攻击风险程度分析**。
  - **IP详情**页签为您展示了该IP地址的**WHOIS值**和**IP反查信息**。
  - **威胁详情**页签为您展示了该IP地址的**威胁标签**列表，包括情报来源、首次发现时间、最后活跃时间和威胁标签。

11.2.3. 配置消费产品

威胁情报集成了威胁监控与大数据分析技术，及时通知您有关威胁情报领域的最新动态。开启消费产品配置功能后，系统会开始监控和收集威胁情报。本文介绍配置消费产品的方法。

操作步骤

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**消费产品配置**。
4. 在**消费产品配置**页面，查看态势感知和Web应用防火墙的数据类型和描述。



数据类型	描述	更新时间
暗网IP	暗网（Tor网络）是一个隐匿的特殊网络环境，暗网的行为与大多数的黑客攻击、黑灰产活动有关	2020年11月29日 08:00:00
恶意域名	木马中控使用的域名、黑客用于传播恶意文件的域名、钓鱼网站域名	2020年11月29日 08:00:00
公共出口IP	通过公共出口IP进行网络访问的用户较多，直接封禁会出现误杀	2020年11月29日 08:00:00
恶意登录IP	黑客进行暴力破解攻击，或者使用后门登录的IP	2020年11月29日 08:00:00
恶意下载源IP	黑客传播木马程序、蠕虫病毒使用的IP地址	2020年11月29日 08:00:00
代理IP	黑客为了隐匿真实IP，会使用代理隐藏自身IP地址	2020年11月29日 08:00:00
中控IP	通过流量协议识别、公开情报获取的中控IP地址	2020年11月29日 08:00:00
矿池IP	挖矿程序需要连接到矿池IP进行通信	2020年11月29日 08:00:00
WEB攻击源IP	历史上发起过WEB攻击的IP	2020年11月29日 08:00:00

5. 在需要开启威胁监控的产品页签，单击**开通状态**开关。

   开通状态开关开启成功后，系统会开始监控和收集产品页签中数据类型对应的威胁情报。

后续步骤

配置成功后，您可以在**总览**页面，查看最近30天内已遭受威胁的整体情况和统计数据。具体操作，请参见查看总览。

11.3. 告警设置

11.3.1. 设置告警联系人

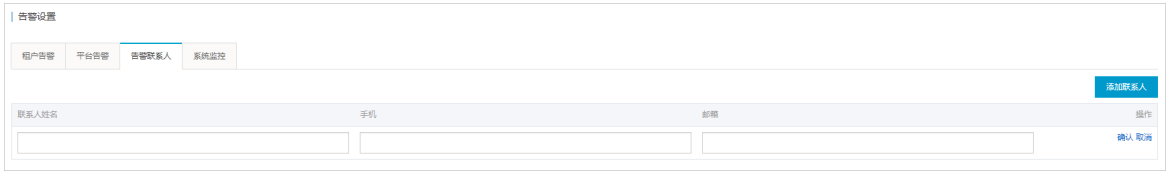
本文介绍如何添加和管理告警联系人。

背景信息

告警联系人是告警消息的接收人，告警消息的发送方式支持手机短信和邮件。当监控数据满足报警规则时，系统自动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. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**告警设置**。
4. 在**告警设置**页面，单击**告警联系人**。
5. 单击**添加联系人**。
6. 填写联系人信息，单击**确认**，添加告警联系人。



7. 管理联系人列表。

   在联系人列表中，单击**编辑**，编辑联系人信息。

11.3.2. 设置告警通知

本文介绍如何设置用户侧和平台侧的各类安全事件的告警通知方式。

背景信息

在**告警通知**中，安全管理员可以配置各种安全事件的告警方式。当发生安全事件时，系统会根据告警方式（邮件或手机短信）通知告警联系人。如何设置告警联系人信息，请参见设置告警联系人。

设置用户侧告警

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**告警设置**。
4. 在**告警设置**页面，单击**租户告警**。
5. 在**告警通知**区域，为各种安全事件选择通知方式。
6. 单击**确认**，完成设置。

设置平台侧告警

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**告警设置**。
4. 在**告警设置**页面，单击**平台告警**。
5. 在**告警通知**区域，为各种安全事件选择通知方式。



6. 单击**确认**，完成设置。

11.4. 升级中心

11.4.1. 升级中心概述

升级中心通过自动和手动方式，进行专有云云盾的系统更新和规则更新等操作，确保专有云及时获取最新的安全保障。

根据专有云的部署环境，升级中心支持规则库通过自动下载和手动导入升级包方式升级。

- 专有云环境和公网互通，可以选择**自动下载安装包**方式。
- 专有云环境和公网不通，可以选择**手动导入升级包**方式。

规则库的升级状态如下所示。

同步状态说明表

状态	说明
待更新	有新版本规则库可以更新。
更新中	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。

11.4.2. 自动检查更新并升级

本文介绍了如何自动检查升级包更新并升级。

背景信息

如果专有云环境可以与公网连通，可以启用自动检查更新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. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**升级中心**。
4. 单击**升级配置**页签。

5. 在**升级配置**页签下，单击**自动更新**页签。
6. 单击**自动更新**后面的按钮开启自动更新，并进行如下配置。



配置说明如下：

配置项	说明
阿里云账号ID	输入阿里云账号ID。
Access Key	输入Access Key。
Access Secret	输入Access Secret。
自动升级时间段	选择自动升级的时间段。支持选择： ○ 0~6时 ○ 0~8时 ○ 0~24时 ○ 22~6时

7. 单击**连通性测试**。
8. 单击**保存**，启用自动检查更新升级包功能。

   启用该功能后，系统能定期下载升级包。

11.4.3. 手动导入升级包并升级

本文介绍如何手动导入升级包并升级。

前提条件

安全管理人员已经获取离线升级包。具体操作，请参见升级包下载。

背景信息

如果专有云环境无法与公网连通，可以通过手动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. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。

3. 在左侧导航栏，单击**升级中心**。
4. 在**升级配置**页签，选择**手动更新**。
5. 手动导入升级包。
   i. 单击**手动导入离线升级包**。
   ii. 在**手动导入离线升级包**对话框中，单击**请选择文件**，选择已下载至本地的离线升级包。
   iii. 单击**确定**。

   文件导入成功后，将显示在**版本更新**页签，可在对应升级列表中，进行升级操作。

11.4.4. 回滚规则库

本文介绍如何回滚库到历史版本。

背景信息

更新后的规则库如果存在问题，可以通过回滚操作将规则库恢复至历史版本，确保不影响业务的运行。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**升级中心**。
4. 单击相应的规则库页签（例如**主机安全**页签）。
5. 在需要回滚规则库的操作栏中，选择**更多 > 回滚**。
6. 在**版本回滚**提示框中，单击**确定**。

11.4.5. 查看历史记录

本文介绍了如何查看规则库的历史版本信息。

背景信息

通过查看规则库的历史记录，了解该规则库的升级记录，如果更新的版本有问题，方便定位问题和回滚到历史版本。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**升级中心**。
4. 单击相应的规则库页签（例如**主机安全**页签）。
5. 在某个规则库的**操作**栏中，单击**历史记录**。

   在**历史升级记录**中可以查看该规则库的升级记录。单击**详情**，查看升级包详情。

11.4.6. 升级包下载

当您需要升级混合云云盾产品的规则库或版本时，您可以在云安全中心下载混合云云盾产品对应版本的升级包，然后上传至云盾控制台，完成混合云云盾产品的版本升级。本文介绍混合云云盾产品的升级模式以及不同升级模式下如何下载版本升级包。

升级模式介绍

云安全中心提供了两种升级模式：普通模式和高级模式。两种升级模式的介绍如下表。

升级模式	描述	具体操作
普通模式	普通模式下，系统会根据您输入的云盾版本标识符，计算出本次更新所需的升级包，并将这些升级包封装成一个组合升级包供您版本升级使用。 选择普通模式，您无需关注本次升级需要下载哪些升级包，系统会自动为您计算并组合本次升级所需的升级包。推荐您使用普通模式快捷地升级混合云云盾产品。 **注意** 云盾V3.12、V3.13、V3.14版本不支持版本标识符，可在版本标识符输入框中输入V3.12、V3.13或V3.14，以获取相应的升级包。	普通模式
高级模式	高级模式下，您可以选择云盾版本号，获取该版本已发布的最新的升级包。您可以根据您的业务需求，有选择地下载升级包进行云盾产品版本升级。 **说明** 高级模式下，您需要明确各升级包之间的依赖关系和升级顺序。	高级模式

普通模式

1. 登录云安全中心控制台云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 升级包下载**。
3. 在**升级包下载**页面的**升级模式**区域，单击**普通模式**。
4. 在**云盾版本标识符**的输入框中，输入要升级版本的混合云云盾的版本标识符，然后单击右侧的**获取规则包**，获取混合云云盾产品的版本升级包。

   说明
   - 您可以单击输入框下方的**获取方式说明**，了解如何获取云盾版本标识符。
   - 云盾V3.12、V3.13、V3.14版本不支持版本标识符，可在版本标识符输入框中输入V3.12、V3.13或V3.14，以获取相应的升级包。
5. 在**升级包下载**区域的升级包列表中，在目标产品升级包**操作**列单击**下载**，下载对应的升级包。
   升级包下载完成后，将升级包上传至云盾控制台，在云盾控制台上继续进行升级相关的操作，完成混合云云盾产品的版本升级。

高级模式

1. 登录云安全中心控制台云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 升级包下载**。
3. 在**升级包下载**页面的**升级模式**区域，单击**高级模式**。
4. 在**云盾版本标识符**区域的左侧的下拉菜单中，选择混合云云盾的版本；在右侧的下拉菜单中，选择您要下载的升级包的版本。
5. 在**升级包下载**区域的升级包列表中，您可以按照您的业务需求，在目标产品升级包**操作**列单击**下载**，下载对应的产品升级包。
   产品升级包下载完成后，将升级包上传至云盾控制台，在云盾控制台上继续进行升级相关的操作，完成混合云云盾产品的版本升级。如果想要完成整个产品的版本升级，你可以下载该产品的所有升级包，然后将所有升级包都上传至云盾控制台，完成整个产品的版本升级。

11.5. 全局设置

11.5.1. 流量采集网段设置

11.5.1.1. 添加流量采集网段

本文介绍了如何添加流量采集网段，该网段是云盾流量安全监控模块的网段范围。

背景信息

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。

> **说明**
> - 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。
> - 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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页面，单击**流量采集网段设置**页签。
5. 单击**添加**。
6. 在**添加监控网段**对话框中，设置监控网段参数。



- **网段**：填写流量采集网段。

  > **说明** 所填写的网段必须是合法网段，并且不允许重复添加。

- **区域**：设置数据中心的区域。

7. 单击**确定**，完成添加。

11.5.1.2. 管理流量采集网段

本文介绍了如何修改和删除流量采集网段。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页面，单击**流量采集网段设置**页签。
5. 选择区域，输入查询网段，单击**查询**。

   在查询结果中，可以查看流量采集网段和区域信息。
6. 在某一网段的**操作**栏中，管理流量采集网段。
   - 修改流量采集网段：

     单击**修改**，修改流量采集网段所属区域。
   - 删除流量采集网段：

     单击**删除**，可删除该流量采集网段。

11.5.2. 区域设置

11.5.2.1. 添加区域网段

本文介绍了如何添加区域网段，该区域指安骑士模块上报检测的区域。

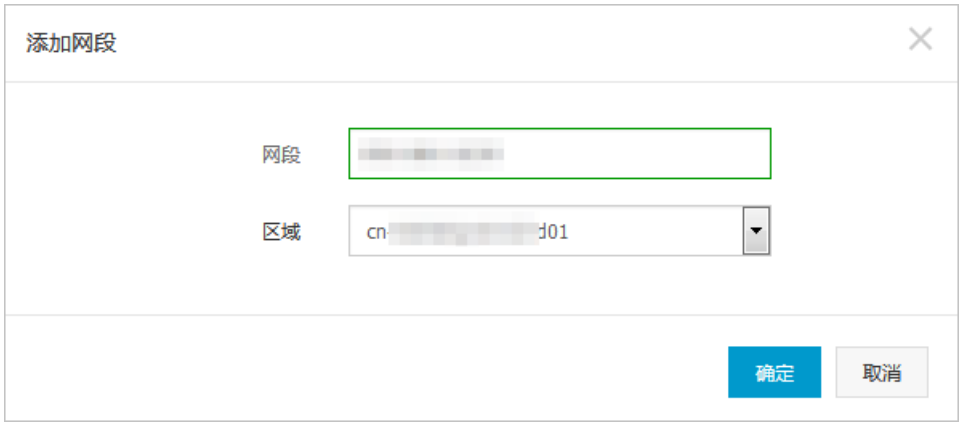
背景信息

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。

> **说明** 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。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页面，单击**区域设置**页签。
5. 单击**添加**。
6. 在**添加网段**对话框中，设置网段参数。



   - **网段**：填写区域对应的网段。

     > **说明** 所填写的网段必须是合法网段，并且不允许重复添加。

   - **区域**：选择所属区域。
7. 单击**确定**，完成添加。

11.5.2.2. 管理区域网段

本文介绍了如何修改和删除区域网段。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页面，单击**区域设置**页签。
5. 选择区域，输入查询网段，单击**查询**。

   在查询结果中，查看区域网段信息。
6. 在某一区域的**操作**栏中，管理区域网段。

- 修改区域网段：

  单击**修改**，修改区域网段信息。

- 删除区域网段：

  单击**删除**，删除该区域网段信息。

11.5.3. 配置白名单

本文介绍了如何配置安骑士中的暴力破解白名单和态势感知中的主机暴力破解白名单、应用攻击白名单、Web攻击白名单。

背景信息

在使用态势感知的安全阻断功能或者主机安全的异常登录功能时，如果存在安全误报，则可以通过白名单功能消除误报。

> **说明** 为了防止安全隐患，请确保白名单中的IP为可信的地址。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页面，单击**白名单设置**页签。
5. 单击**添加**。
6. 在**添加白名单**对话框中，设置白名单参数。



参数	说明

参数	说明
类型	◦ **全局登录白名单**：符合此类型的白名单，安骑士将不会上报暴力破解事件和异常登录事件。 ◦ **暴力破解白名单**：符合该类型的白名单，安骑士将不会上报暴力破解事件。
源IP	访问来源的IP或者IP段。
目的IP	访问目的的IP或者IP段。

7. 单击**确定**。
   白名单添加成功后，单击**删除**并在**删除白名单**对话框中单击**确定**，可删除已不需要的白名单。

11.5.4. 配置拦截策略

本文介绍了如何启用应用攻击阻断和暴力破解阻断功能。

背景信息

通过安全阻断功能，能够防御Web攻击和暴力破解。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**页面，单击**拦截策略设置**页签。
5. 单击**Web攻击阻断**和**暴力破解阻断**操作栏下的开关，启用**应用攻击阻断**和**暴力破解阻断**功能。



> **说明**
>
> 操作栏中，红色状态表示该功能关闭，绿色状态表示该功能开启。
>
> 关闭后，相应的拦截功能将被禁用，仅提供预警功能。

11.5.5. 一键封禁

您可以通过一键封禁功能手动封禁风险目标。

操作步骤

1. 登录云盾安全中心。

2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**界面，单击**一键封禁**页签。
5. 单击页面右侧的**添加**。
6. 在**添加**对话框中，设置风险目标。



参数	说明
协议类型	设置协议类型，可选值：**IPv4**、**IPv6**。
源IP	设置封禁的源IP地址。
目的IP	设置封禁的目的IP地址。
目的端口	设置封禁的目的IP地址端口。
禁封时长	选择封禁的时长，可选**1天**、**7天**和**30天**。
类型	设置封禁类型，可选**白名单**和**黑名单**。
备注	输入封禁原因的描述信息。

7. 单击**确定**。

11.5.6. 自定义IP地理位置设置

11.5.6.1. 添加自定义IP地理位置

本文介绍了如何添加自定义IP地址和自定义地理位置，您可根据组网规划自定义内部IP地址，避免通用地址库的IP地址匹配到境外国家地址。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**界面，单击**自定义IP地理位置**页签。
5. 单击**添加**。

   如果需要添加多个IP地址和地理位置，可单击**批量上传（.txt文件）**将IP地址和地理位置通过模板批量导入。
6. 在**新增**对话框中，设置自定义IP地址和地理位置。



7. 单击**确定**，完成添加。

11.5.6.2. 管理自定义IP地理位置

本文介绍了如何修改和删除自定义IP地址和自定义地理位置。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**全局设置**。
4. 在**全局设置**界面，单击**自定义IP地理位置**页签。
5. 在需要管理的IP地址的**操作**栏中，管理自定义IP地址和地理位置。
   - 修改：

     单击**编辑**，在弹出的**编辑**对话框中，可修改自定义的地理位置。
   - 删除：

单击**删除**，在弹出的**删除**对话框中，单击**确认**，即可删除自定义IP地理位置。

11.6. 系统监控

11.6.1. 配置云防火墙的引流网段

在使用云防火墙之前，需要配置云防火墙的引流网段。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击 **系统监控**。
4. 在**系统监控**页面**服务监控**区域的**云防火墙ICFW**页签，单击**引流配置 - 业务网段**右侧的**添加**。
5. 在**添加**对话框中，设置**设置集群ID**、**引流网段**和**类型**，并填写**业务描述**。



6. 单击**确定**，完成引流网段的配置。
   配置完成后，可以在**ISW引流配置 - 业务网段**、**服务自检状态**和**接口状态**中查看相关信息。

11.6.2. 系统巡检

本文介绍如何对云盾控制台中云防火墙、流量安全监控等系统进行系统巡检，监控系统服务状态和功能。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击 **系统监控**。

4. 在**网络安全**页签的**系统巡检**区域，对巡检列表中系统进行系统巡检。



系统支持批量巡检或巡检单产品，操作如下所示：

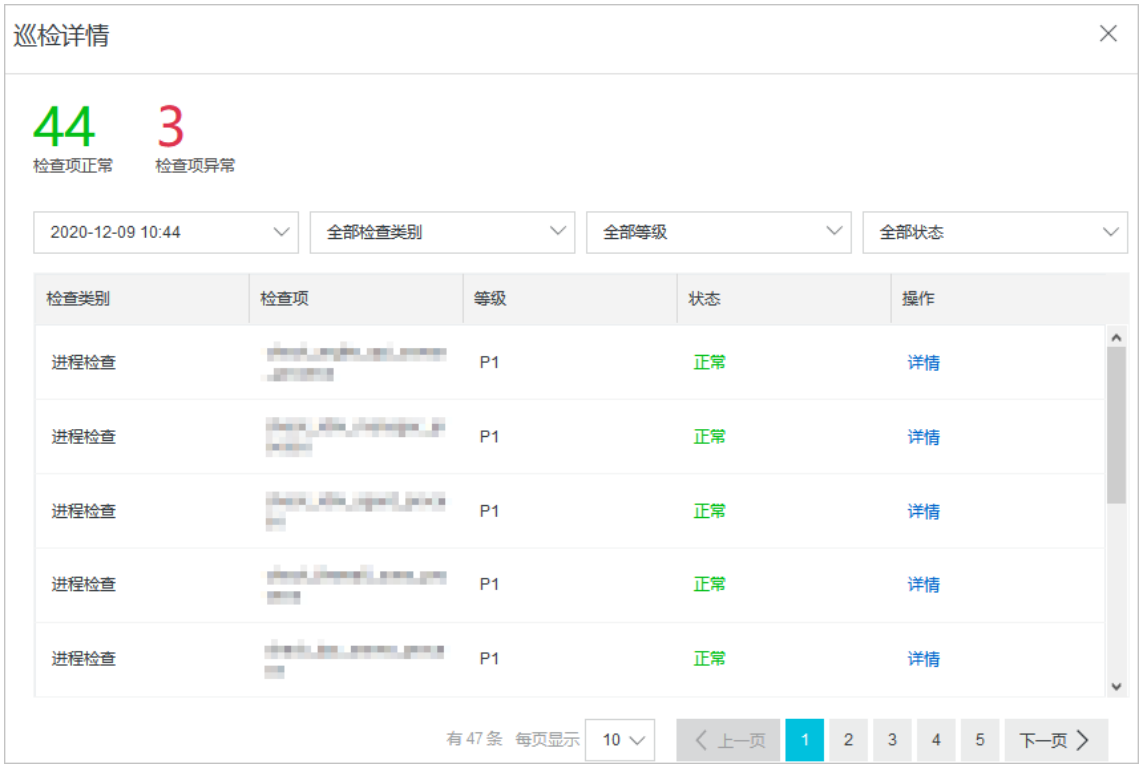
- 批量巡检：在**系统巡检**区域，单击**一键巡检**，对巡检列表中所有系统启动巡检。
- 巡检单产品：在**系统巡检**区域的巡检列表中，单击需要巡检系统**操作**列的**立即巡检**。

巡检成功后，巡检列表的**巡检状态**为**已完成**。

5. 查看系统的巡检结果。

查看内容如下所示：

- 在巡检列表中，查看系统名称、最近巡检时间、巡检项数量、正常项数量、异常项数量、巡检状态。
- 单击巡检系统**操作**列的**详情**，在**巡检详情**页面查看正常项数量、异常项数量和检查项详情列表。



- 单击巡检系统**操作**列的**下载**，根据提示信息将巡检结果下载到本地查看和备份。

11.7. 账号管理

11.7.1. 查看和修改专有云账号

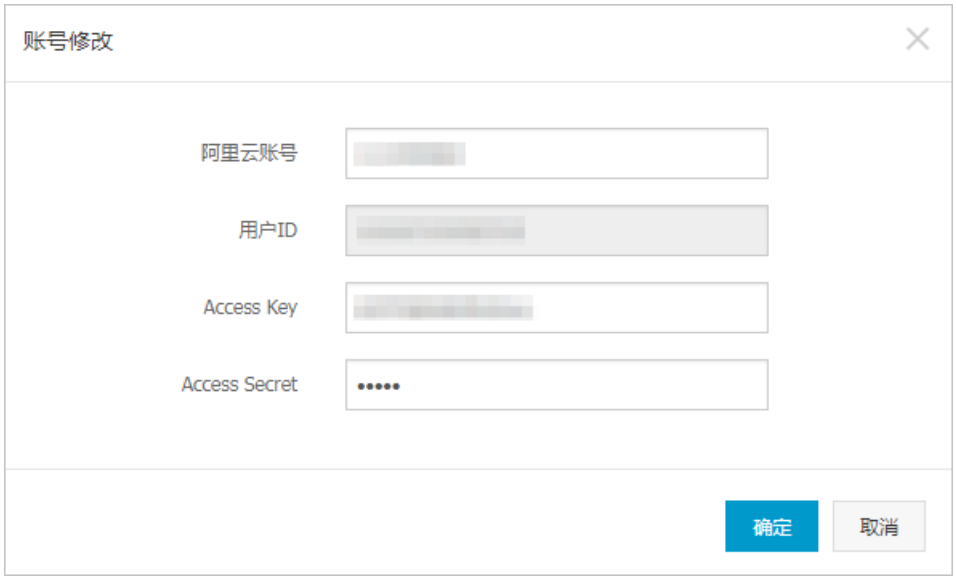
本文介绍查看、修改系统绑定的专有云账号信息。

背景信息

> **说明** 云盾中的资产均与账号绑定，请谨慎修改。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**账号管理**。
4. 在**账号管理**页面，单击**专有云账号**页签。
5. 修改阿里云账号信息。
   i. 单击**修改**。
   ii. 在**账号修改**对话框中，修改账号信息。



   iii. 单击**确定**。
6. 查看阿里云账号详情。

   单击**详情**，查看阿里云账号详细信息。



11.7.2. 添加公共云账号

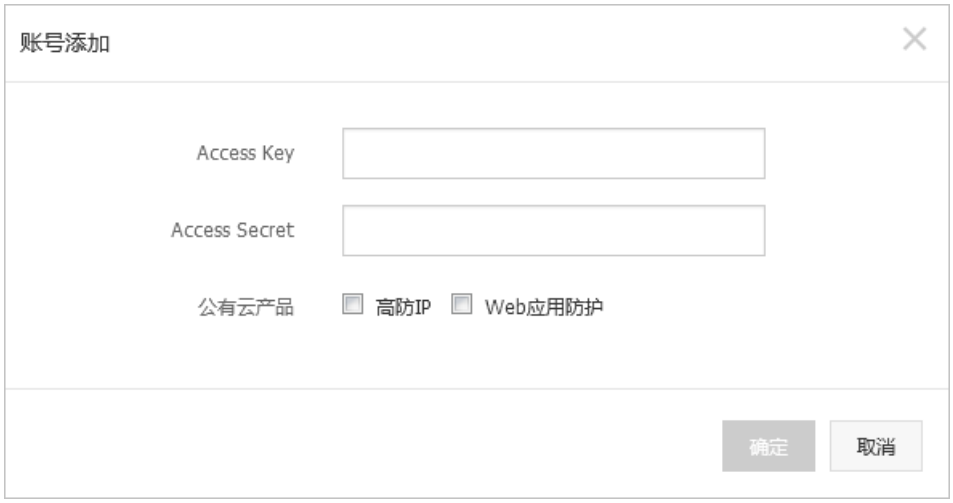
如果专有云中需要使用混合云功能，需要根据本文添加阿里云公共云账号。

背景信息

通过在专有云中添加公共云账号，您可以在专有云中管理该公共云账号下已购买的高防IP和WAF，实现混合云功能。

操作步骤

1. 登录云盾安全中心。
2. 在控制台右上方，单击**安全**，在**全局平台安全**区域单击**云盾**。
3. 在左侧导航栏，单击**账号管理**。
4. 在**账号管理**页面，单击**公有云账号**页签。
5. 在**控制台集成**页签下，单击右侧**添加**。
6. 在**账号添加**对话框中，设置公共云账号信息和使用的公共云产品。



- 输入阿里云公共云账号的**Access Key**和**Access Secret**。
- 选择使用的公共云产品，支持**高防IP**和**Web应用防护**，可单选一个产品或全选。

7. 单击**确定**。

执行结果

添加成功后，新添加账号会在**公共云账号**列表中显示。如果账号变更或不需要使用，您可以进行**修改**和**删除**操作。

11.8. 安全监控

云盾控制台可以监控云盾各安全产品的水位线，便于提前发现产品性能瓶颈，及时进行扩容或降级处理，预防系统发生故障。本文介绍如何查看云盾控制台各产品安全信息及如何管理监控项。

整体系统监控

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**安全监控**。
4. 在**安全监控**页签，查看云盾控制台各安全产品的整体信息和安全产品监控列表。



在**整体系统监控**页签左上方，可以查看安全产品的整体信息，如下所示：

- **监控产品类**：云盾控制台监控的安全产品总数量。
- **监控项**：监控项总数。
- **异常项**：监控项中状态异常的项目数量。

在安全产品监控列表，可以查看的信息如下所示：

项目	说明
产品	云盾控制台监控的安全产品名称。
监控指标	监控的安全产品指标。
描述	安全产品指标的描述信息。
监控项数	安全监控指标中监控项目的数量。
异常数	监控项中状态异常的项目总数及各紧急程度的异常项数量。 通过颜色区分异常项紧急程度，红色表示紧急异常，橙色表示严重异常，蓝色表示一般异常。 紧急P1 严重P2 一般P3

项目	说明
状态	监控指标运行状态。

5. 单击监控指标**操作**列的**详情**，在**监控详情**面板查看监控项的详细信息。



在**监控详情**面板左上方，可以查看监控项的整体信息，如下所示：

- **总监控项**：安全监控指标中的监控项总数。
- **正常项**：正常状态的监控项总数。
- **异常项**：异常状态的监控项总数。

在监控项列表中，可以查看的信息如下所示：

项目	说明
监控项	安全监控指标的监控项名称。
报警阈值	监控项状态变为异常的阈值。
持续时间	监控项达到阈值的持续时间后，状态变为异常。
监控等级	监控项异常时报警的紧急程度。
状态	监控项的状态。
告警通知	监控项异常时，开启或关闭**告警通知**的开关。 开关状态变为  图标时，当监控项异常时会发送告警通知。

管理监控项

1. 登录云盾安全中心。
2. 在左侧导航栏，选择**云安全管理中心（SOC） > 规则运营**。
3. 在左侧导航栏，单击**安全监控**。
4. 在**安全监控**页签的监控指标列表，单击监控指标**操作**列的**详情**。
5. 在**监控详情**面板的监控项列表，单击**操作**列的**调整阈值**、**处理**或**调整持续时间**，管理监控项。

   可对监控项做如下配置：

- **调整阈值**：在**调整阈值**页面，设置监控项最新阈值，单击**确定**。



调整成功后，当监控项达到最新阈值时报警。

- **处理**：异常监控项可根据实际需要设置监控项状态，操作如下：
  - 当监控项告警无需处理时，可在下拉列表中选择**忽略**。设置成功后，监控项的状态为**已忽略**。
  - 当监控项告警处理完成后，可在下拉列表中选择**已处理**。设置成功后，监控项的状态为**已处理**。
- **调整持续时间**：在**调整持续时间**页面，设置最新持续时间，单击**确定**。



调整成功后，按照最新持续时间监控产品监控项。