Hillstone®
山 石 网 科

智源智能安全运营平台 WebUI用户手册

Version V2.0R7



TechDocs | docs.hillstonenet.com

Copyright 2022 Hillstone Networks. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks.

Hillstone Networks

本文档禁止用于任何商业用途。

联系信息

北京

地址：北京市海淀区宝盛南路1号院20号楼5层

邮编： 100192

苏州

地址：苏州高新区科技城景润路181号

邮编：215000

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册介绍山石网科的产品系统的使用方法。

获得更多的文档资料，请访问：https://docs.hillstonenet.com.cn

针对本文档的反馈，请发送邮件到：TechDocs@hillstonenet.com

山石网科

https://www.hillstonenet.com.cn

TWNO: TW-WUG-iSOPV2.0R7-CN-V1.0-Y22M05

目 录

目 录 1

欢迎 1

第1章 部署智源 2

典型部署 2

单机部署 2

集群部署 3

软件化部署 5

部署智源平台（单机） 6

部署智源平台（集群） 9

智源平台单机扩展至集群 10

直接部署智源平台集群 16

部署流量探针 25

部署威胁溯源插件 27

部署环境要求 27

部署方式 27

在用户主机上安装威胁溯源插件（单机安装方式） 28

准备工作 28

安装部署步骤 28

步骤一：使用UpdateMsi工具更新安装程序 28

步骤二：运行msi格式安装程序完成安装 29

步骤三：确认进程 30

卸载威胁溯源插件 30
升级威胁溯源插件 30
在用户主机上安装威胁溯源插件（域安装方式） 31
准备工作 31
使用组策略分配安装威胁溯源插件 32
分配给域用户 32
步骤一：创建组策略对象 32
步骤二：用户配置-编辑组策略部署软件 33
步骤三：将组策略应用到用户组织单位 36
步骤四：强制更新组策略 38
分配给域中的计算机 38
步骤一：创建组策略对象 38
步骤二：计算机配置-编辑组策略部署软件 39
步骤三：将组策略应用到计算机组织单位 42
步骤四：强制更新组策略 43
使用组策略卸载已分发安装的插件 43
使用组策略升级已分发安装的插件 44
部署威胁探针 46
部署山石云鉴 48
软件化部署 50
适用场景 50
产品信息 50
在VMware ESXi上部署软件化智源 50

系统要求和限制 51
部署步骤 51
第一步：访问登录VMware ESXi 6.7平台 51
第二步：创建虚拟机 51
第三步：配置智源访问地址以及部署系统 53
第四步：访问智源系统 54
在CentOS 7系统终端主机上部署软件化智源 54
系统要求和限制 55
准备工作 55
部署步骤 55
第一步：启用虚拟机管理图形化界面 55
第二步：创建并配置虚拟机 56
第三步：配置智源访问地址以及部署系统 60
第五步：访问智源系统 61
在Windows 10系统终端主机上部署软件化智源 61
系统要求和限制 61
部署步骤 62
第一步：启用Hyper-V功能 62
第二步：创建并配置虚拟机 62
第三步：连接并启动虚拟机 66
第四步：配置智源访问地址以及部署系统 66
第五步：访问智源系统 67
集群部署软件化智源 67

激活智源系统 70
通过CLI方式激活 70
通过WebUI方式激活 72
第2章 态势监控 77
关注态势 77
告警 77
安全总览 78
我的关注 80
资产态势 82
威胁事件监控 84
弱点监控 85
系统状态监控 87
资产态势 87
溯源模式 88
全局溯源 89
溯源结果 90
内部资产 91
外部IP/域名/文件MD5 95
无结果 98
流量监控 99
过滤条件 99
流量趋势 100
源IP活动 TOP 10 100

目的IP活动 TOP 10 101
平台总览 102
态势大屏 103
投屏模式自定义配置 109
自定义模块 109
新建自定义模块 110
例：添加看板 112
设置为默认模块 112
多标签页展示 113
第3章 威胁分析 114
威胁 115
全部资产 115
查看资产详细信息 117
服务器列表 118
查看服务器详细信息 120
终端 122
终端列表 122
查看终端详细信息 124
主机列表 126
查看主机详细信息 128
用户列表 130
查看用户详细信息 131
业务列表 133

查看业务详细信息 135
事件列表 136
查看威胁详细信息 139
聚合威胁事件 141
配置聚合威胁事件功能 141
查看聚合威胁事件详细信息 142
清理误报威胁事件 144
日志 146
日志概览 147
Syslog列表 148
NetFlow列表 149
Meta Data列表 149
Sysmon列表 150
Linux列表 151
日志搜索 152
可视化展示 156
创建日志可视化看板 156
第4章 弱点分析 160
弱点分析 162
导入弱点报告 162
主机 162
弱点 164
弱点报告获取 167

查看弱点报告获取任务 167
新建弱点报告获取任务 167
弱点扫描任务 169
查看弱点扫描任务 169
新建弱点扫描任务 170
扫描器配置 173
查看扫描器列表 173
添加扫描器 173
弱点分析配置案例 176
组网场景 176
准备工作 177
配置步骤 177
第5章 风险管理 184
全部资产风险 185
风险状态总览 185
风险资产 186
查看风险资产详情 187
失陷报告 187
风险报告 189
威胁事件 190
弱点 192
服务器风险 194
风险状态总览 194

风险服务器 195
查看风险服务器详情 196
失陷报告 196
风险报告 198
威胁事件 199
弱点 201
终端风险 203
风险状态总览 203
风险终端 204
查看风险终端详情 205
失陷报告 205
风险报告 207
威胁事件 208
弱点 210
业务风险 212
风险状态总览 212
风险业务 213
查看风险业务详情 213
第6章 事件响应 216
剧本管理 216
查看剧本 217
剧本总览 217
查看剧本列表 218

查看待响应任务 220
查看中止任务 221
查看剧本响应记录 223
查看剧本详情 226
配置剧本 227
预定义剧本 228
创建剧本 229
配置剧本基础信息 232
配置剧本触发条件 233
配置威胁情报库动作 236
配置判定条件 237
配置网络安全设备动作 240
配置策略 240
配置IP阻断 243
配置主机安全设备动作 244
配置访问控制 244
配置结束进程 246
配置隔离文件 248
配置重启终端 249
配置平台动作 251
创建工单 251
发送邮件 253
联动实体 255

联动实体动作 257
网络安全设备 257
添加网络安全设备实体 259
查看网络安全设备实体策略/IP阻断信息 263
配置策略 265
配置IP阻断 268
主机安全设备 269
添加主机安全设备实体 271
查看主机安全设备实体详情信息 271
配置访问控制 272
配置结束进程 274
配置隔离文件 274
配置重启终端 275
配置阻止非信任USB 276
配置USB白名单 277
威胁情报库 278
添加威胁情报库实体 280
工单管理 281
新建工单 282
查看工单详情 284
第7章 报告管理 286
报告总览 287
生成报告 287

报告任务 290
新建报告任务 290
报告模板 293
自定义报告Logo 294
查看报告模板详情 295
新建自定义报告模板 297
编辑自定义报告模板 299
删除自定义报告模板 299
等保管理 300
等保系统 300
创建等保系统 300
编辑等保系统 301
删除等保系统 302
管理资产 302
创建新资产 302
导入资产 304
下载模板 304
导入资产 304
管理等保流程 305
创建等保流程 305
编辑等保流程 305
定级阶段 305
备案阶段 307

自查阶段 308
整改阶段 310
等级测评阶段 311
监督检查阶段 313
删除等保流程 314
查看等保系统/流程 314
第8章 情报中心 316
热点威胁资讯 317
威胁情报库 320
威胁情报库升级 320
在线升级 320
离线升级 320
自定义威胁情报管理 321
白名单 321
全局白名单 321
查看全局白名单 321
手动添加全局白名单 323
下载全局白名单模板 324
导出全局白名单 325
导入全局白名单 326
DNS类白名单 326
查看DNS类白名单 327
手动添加新域名至DNS类白名单 328

下载DNS类白名单模板 328
导出DNS类白名单 329
导入DNS类白名单 330
文件类白名单 330
查看文件类白名单 330
添加文件类白名单 332
下载文件类白名单模板 332
导出文件类白名单 333
导入文件类白名单 333
黑名单 334
查看黑名单 334
添加新情报至黑名单 335
第9章 资产管理 337
资产管理 338
资产总览 338
资产列表 339
查看资产详情 340
编辑资产 343
资产配置 347
新建资产 348
新建资产组 350
下载模板 353
导出资产或资产组 353

导入资产或资产组 354
错误提示 356
终端用户状态 357
资产探测 359
新建资产探测任务 360
区域管理 363
新建区域 364
下载模板 365
导出区域 366
导入区域 366
错误提示 367
业务管理 369
新建业务 370
下载模板 371
导出业务 372
导入业务 372
错误提示 373
待入库资产 375
被动发现 375
待入库资产 375
已忽略资产 376
主动探测 377
待入库资产 377

已忽略 378
入库记录 379
待更新资产 381
待更新资产 381
更新记录 382
第10章 引擎管理 384
威胁引擎 385
默认引擎 385
编辑默认规则 387
配置保护对象 388
编辑弱密码检测规则 388
关联分析 390
新建自定义规则 392
攻击链引擎 402
默认引擎 402
编辑默认规则 403
关联分析 405
新建自定义规则 406
第11章 日志管理 408
日志源管理 409
新建日志源 409
日志解析 411
日志解析配置 412

日志解析配置特征库升级 412
在线升级 412
离线升级 413
新建自定义日志解析配置 413
新建日志解析模板 414
配置日志解析流程 416
配置Grok解析流程 417
配置Key-Value解析流程 420
配置JSON解析流程 423
调整解析流程顺序 425
配置日志标准化 425
查看日志解析配置 428
配置日志解析规则 430
新建自定义日志解析规则 430
查看日志解析规则 432
日志存储管理 434
查看存储空间 434
查看日志备份 434
导入备份日志 434
查看已恢复的日志备份 435
日志备份配置 436
自动备份 436
手动备份 437

FTP配置 438
新建FTP服务器 438
查看FTP配置列表 440
日志设备 441
日志服务器 442
新建日志服务器 442
第12章 系统设置 444
系统信息 446
查看系统信息 446
权限设置 448
用户配置 448
新建用户 448
删除用户 450
修改用户密码 450
可信主机 451
新建可信主机 452
联系人管理 454
新建联系人 455
系统日志 457
日志的严重等级 457
事件日志 458
操作日志 459
日志设置 460

升级管理 461
系统版本升级 461
安全设置 462
登录策略 462
登录超时 462
用户锁定 463
密码策略 463
配置密码规则 463
开启/关闭新用户强制修改密码 464
配置密码强制修改周期 464
密码过期告警 465
许可证管理 466
许可证展示 466
申请许可证 466
安装许可证 467
通讯配置 469
邮件服务器 469
新建邮件服务器 469
短信网关 470
配置短信网关 470
告警通知 471
告警通知设置 473
查看告警通知规则 473

编辑自动告警通知规则 475
默认设置 475
关注事件告警规则 475
高危严重事件告警规则 477
编辑自动告警通知规则 479
新建威胁告警通知规则 482
新建系统告警通知规则 486
查看告警通知 490
查看告警通知信息 490
查看许可证过期信息 491
网络管理 492
接口配置 492
编辑接口信息 492
网络配置 493
证据信息管理 495
探针管理 497
流量探针 497
威胁探针 497
级联管理 499
级联设置 499
编辑级联设置 500
下级平台管理 502
上级平台管理 503

基础配置 503
编辑上级平台信息 504
上报数据配置 505
集群管理 506
安全分析计划 507
启用/禁用安全分析计划 507
人行数据对接 508
数据对接配置 508
开启/关闭人行数据对接功能 508
基础配置 508
上报数据配置 511
数据对接历史 513
恢复出厂设置/退出/重启/关机 515
恢复出厂设置 515
退出登录 515
重启系统 515
关机 515

欢迎

感谢您选择山石网科产品！

以下内容可以帮助您了解如何操作山石网科的产品：

新手入门指南

- 《智源智能安全运营系统新手入门指南》（PDF下载）

系统操作手册

- 《智源安全运营平台WebUI用户手册》（PDF下载）
- 《智源流量探针WebUI用户手册》（PDF下载）

典型案例

- 《智源智能安全运营系统配置案例手册》（PDF下载）

部署手册

- 《山石网科智源智能安全运营系统部署手册》（PDF下载）

硬件安装手册

- 《智源安全运营平台硬件参考指南》（PDF下载）
- 《智源流量探针硬件参考指南》（PDF下载）

其他支持：

- 官方网站: https://www.hillstonenet.com.cn
- 手册下载：https://docs.hillstonenet.com
- 技术支持：400-828-6655

第1章 部署智源

山石智源智能安全运营系统，是全息数据驱动的AI分析运营系统，由分析平台与丰富的探针共同构成，可为各行业客户提供网络威胁分析、态势呈现与溯源等功能，解决客户监控盲区，潜在安全隐患、运维低效等问题。智源具备全息数据采集的能力，通过多种类型的数据探针采集数据，基于海量网络流量、威胁事件和终端日志等进行智能数据挖掘及分析，呈现全局网络安全及威胁态势，并支持多维度投屏展示、联动响应、工单响应等核心功能，让企业安全运营尽在掌握之中。

目前智源支持6种类型的数据源，分别来自于网络设备、流量探针、威胁探针、Linux系统设备、用户主机以及山石云鉴，具体信息如下：

- 网络设备：将网络设备（如防火墙设备、IDPS设备、WAF设备）的Syslog信息、NetFlow信息发送至智源平台。
- 流量探针：将网络设备的流量镜像到探针设备，再将解析、分析、提取后的元数据（Meta Data）或NetFlow信息发送至智源平台。
- 威胁探针：威胁探针设备对收到的镜像流量检测、监测以及分析后，再将产生的威胁信息以Syslog日志形式发送至智源平台。
- Linux系统设备：将Linux系统的设备产生的日志通过syslog协议发送到智源平台。
- 用户主机：通过威胁溯源插件将采集到的主机进程创建、网络访问、文件操作、注册表修改等相关行为信息（Sysmon）发送至智源平台。
- 山石云鉴主机安全管理系统（CloudDis）：将山石云鉴主机安全管理系统的资产信息、风险行为信息以Syslog日志的形式发送至智源平台。

典型部署

智源的典型部署主要包含智源平台、流量探针、威胁探针、威胁溯源插件、山石云鉴五部分。

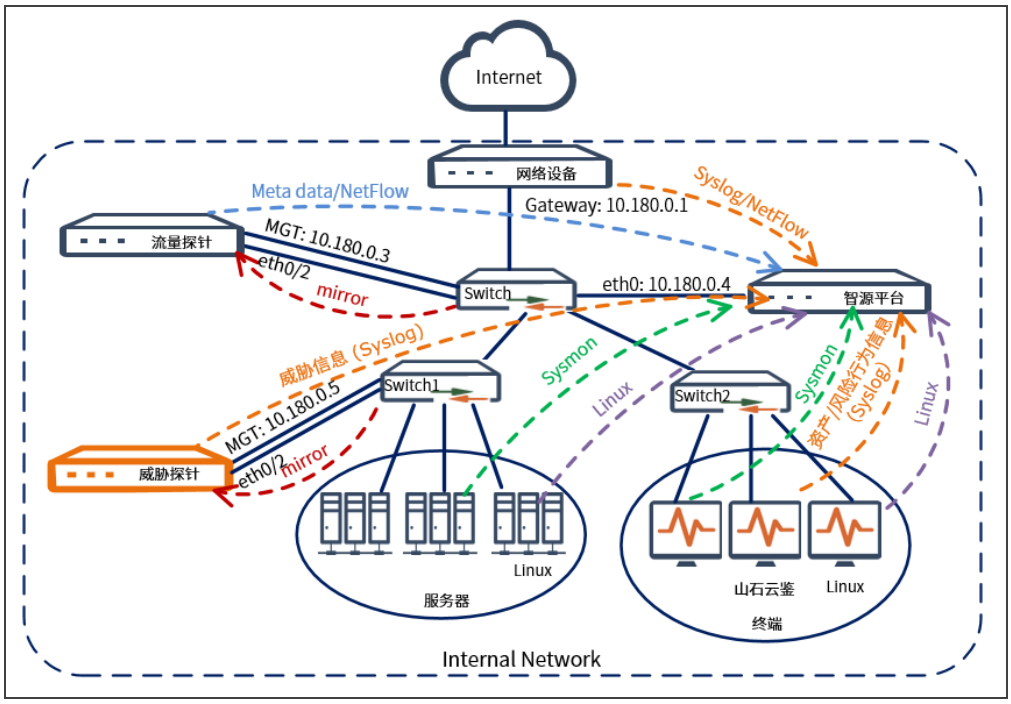
智源平台的典型部署包含单机部署、集群部署两种方式。

单机部署

智源平台（单机）、威胁探针和流量探针部署在用户内网环境中，威胁溯源插件部署在用户服务器或终端上以及山石云鉴作为终端部署在内网中。部署完成后，智源平台可以接收来自流量探针、威

胁探针、Linux系统设备、网络设备、山石云鉴以及用户服务器和终端的信息（Meta Data、Syslog、NetFlow、Linux、Sysmon、威胁信息、资产信息、风险行为信息），从而对全网进行监控和分析。

您可以参考以下单机部署场景进行部署。下图中的网络设备以防火墙为例。



按照以下步骤进行部署：

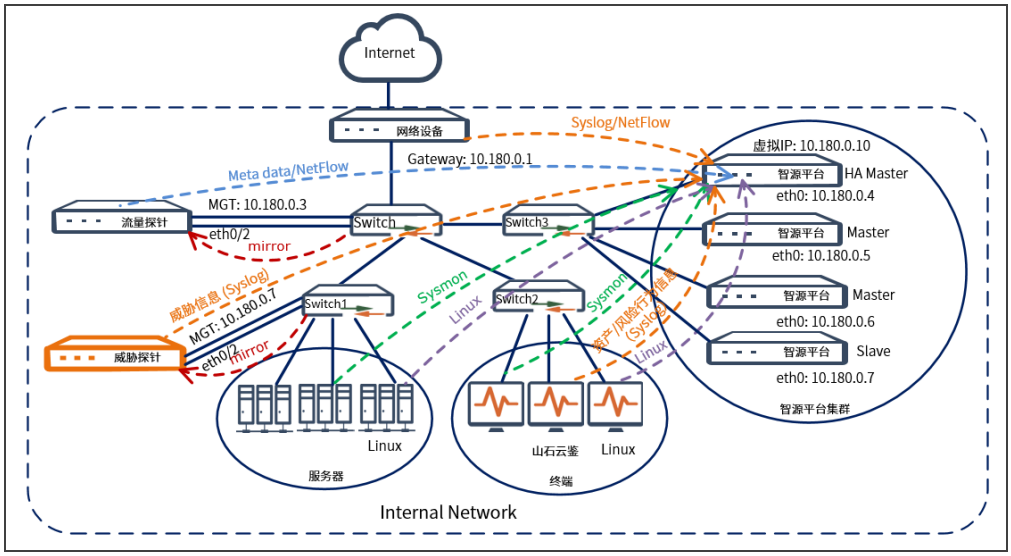
1. "部署智源平台（单机）" 在第6页
2. "部署流量探针" 在第25页（可选）
3. "部署威胁溯源插件" 在第27页（可选）
4. "部署威胁探针" 在第46页（可选）
5. "部署山石云鉴" 在第48页（可选）

集群部署

随着用户数据量的增加，单台智源平台可能无法满足用户的需求。针对这一问题，智源平台支持集群部署，即用户可以部署多台智源平台，进而缓解单台智源平台的数据量压力。

当集群中智源平台的数量大于或等于3台时，智源平台集群将默认支持高可靠性（HA），能够在设备产生故障时提供备用方案。当集群中一台智源平台发生故障不可用时，集群中其他智源平台将会继续接收以及处理数据，从而保证数据通信的不间断，有效增强网络的可靠性。

参考如下集群部署拓扑图，智源平台（集群）、流量探针和威胁探针部署在用户内网环境中，威胁溯源插件部署在用户服务器和终端上，以及山石云鉴作为终端部署在内网中。集群中所有智源平台都部署在同一个二层网络中，第一台部署的智源平台作为HA Master，HA Master会根据其配置的内部IP网段（地址）为其他智源平台分配可用的内部IP地址。部署完成后，HA Master可以接收所有来自流量探针、威胁探针、Linux系统设备、网络设备、山石云鉴以及用户服务器和终端的信息（Meta Data、Syslog、NetFlow、Linux、Sysmon、威胁信息、资产信息、风险行为信息），再将数据信息通过内部IP地址分发给集群中其他智源平台。下图中的网络设备以山石网科防火墙为例。



按照以下步骤进行部署：

1. "部署智源平台（集群）" 在第9页
2. "部署流量探针" 在第25页（可选）
3. "部署威胁溯源插件" 在第27页（可选）
4. "部署威胁探针" 在第46页（可选）
5. "部署山石云鉴" 在第48页（可选）

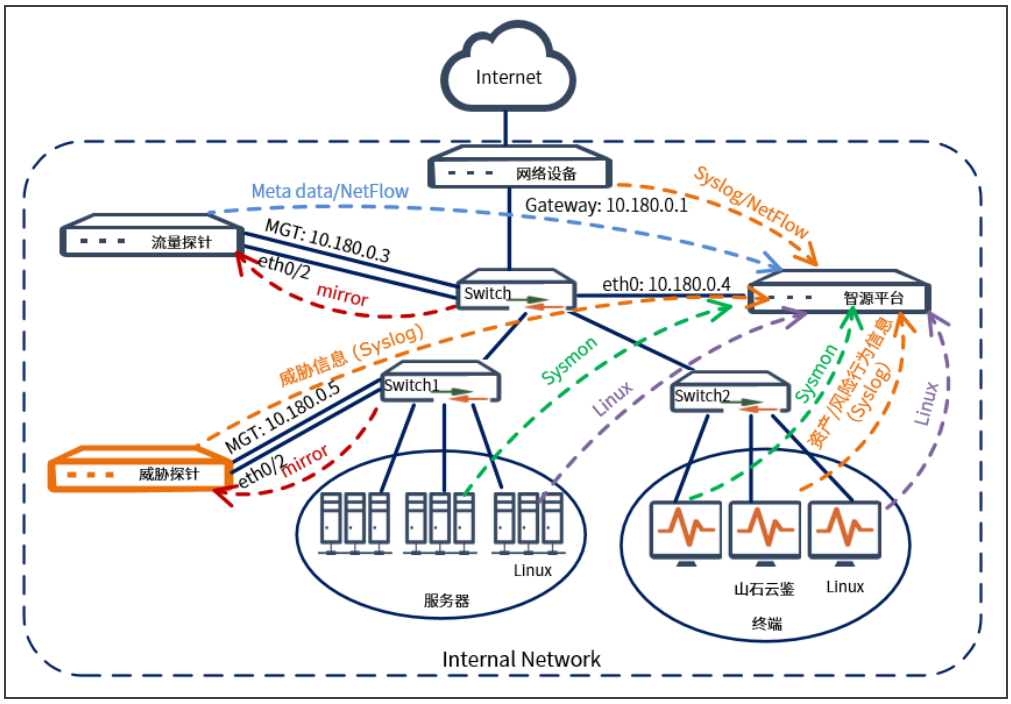
软件化部署

软件化部署，是指将智源平台作为一个纯软件形态的产品，部署及运行在终端主机、虚拟机上。详细部署方式，请参阅"软件化部署" 在第50页。

部署智源平台（单机）

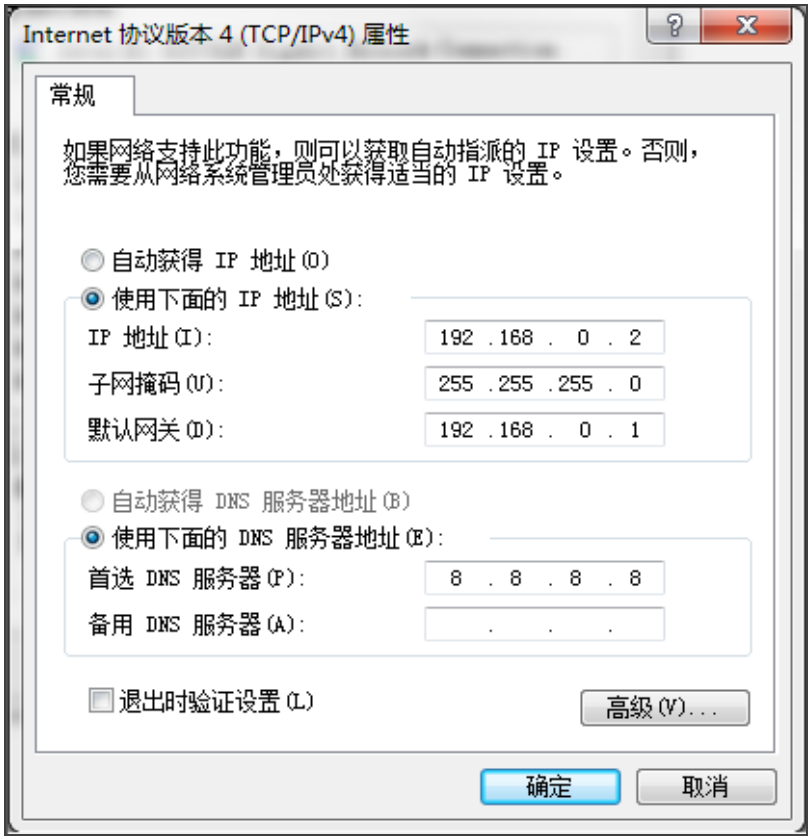
智源平台接收来自流量探针、威胁探针、Linux系统设备、网络设备、山石云鉴以及用户服务器和终端的信息（Meta Data、Syslog、NetFlow、Linux、Sysmon），从而对全网进行监控和分析。

您可以参考以下单机部署场景进行部署。



部署单机智源平台，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、SSH版本为“SSH2”、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network internal segment**命令检查系统内部IP地址是否和用户网络中的IP地址冲突。如果不冲突，保持当前系统内部IP地址；如果冲突，输入**network internal segment --ip** *subnet/mask* 命令配置网段（掩码必须小于24，例如192.168.82.0/23），系统将会自动分配内部IP地址。

   注意：请确保该步骤在部署智源平台系统之前进行。在系统部署完成后，请尽量不要修改当前系统的内部IP地址。

6. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

7. 为eth0接口配置IP地址，输入以下命令：

   `SG-6000#network ipconfig --interface eth0 --ip 10.180.0.4/24`

   （如智源平台为IPv6类型的IP地址，可使用`SG-6000#network ipv6config --interface eth0 --ipv6 X:X:X:X::X/ipv6-prefix`）。

8. 配置默认网关，输入以下命令：

   `SG-6000#network routeconfig --dst 0.0.0.0/0 --gateway 10.180.0.1`

   （如使用IPv6类型的IP地址，配置默认网关可使用`SG-6000#network routev6config --dst ::/0 --gateway X:X:X:X::X`）

9. （可选）如果有多网段管理需求，则为另一个link状态为true的接口配置IP地址，方法同步骤7。

   注意：智源平台只能存在一个默认网关，因此为了使多网段网络均能正常通信，应根据实际网络拓扑和需求配置相应的路由，方法同步骤8。

10. 输入**show network ipconfig**和**show network routeconfig**命令检查当前接口和路由配置。

11. 输入**deploy standalone**命令并选择系统语言部署智源平台系统。

    注意：系统语言选定后如需修改，请reset设备并重新部署智源平台系统。

12. 部署完成后，打开Web浏览器，在地址栏中输入https://10.180.0.4并按回车键。

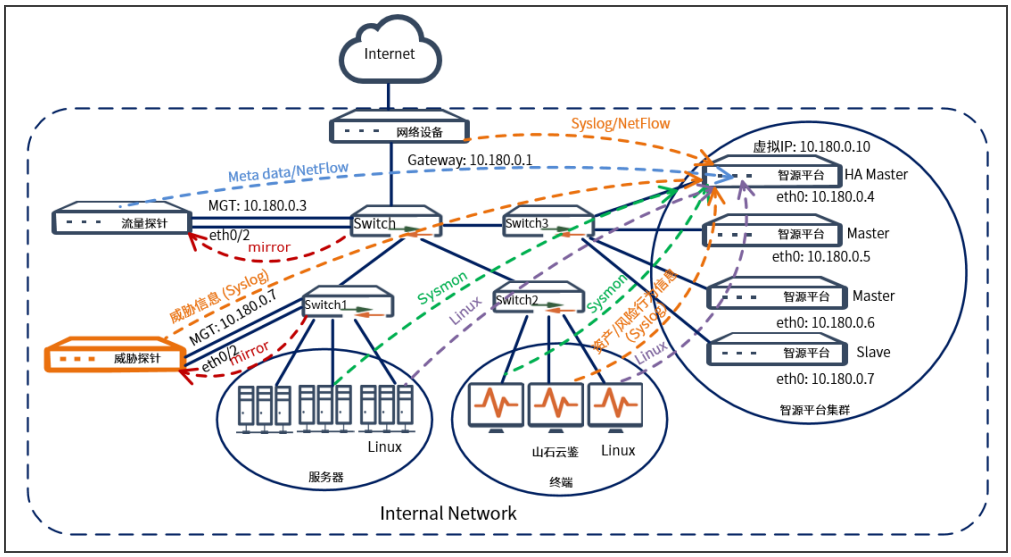
13. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。



注意: 使用默认用户名和密码初次登录后，建议立即修改默认密码。

部署智源平台（集群）

您可以参考以下集群部署场景进行部署。



注意:

- 目前，集群最多支持部署5台智源平台。
- 当集群中部署2台智源平台时，则不支持HA功能，且系统版本必须为2.0R1或以上版本。
- 如需要使用集群的HA功能，请确保集群中智源平台系统版本为2.0R3或以上版本。从低版本升级后，需要重新部署以保证集群HA功能生效。
- 集群中的所有智源平台信息和软件版本必须保持一致。
- 集群中的智源平台必须部署在同一个二层网络中。
- 确保配置的内部IP地址网段中的IP地址数量超过集群中的设备总数。
- 建议安装万兆板卡，并使用万兆网口进行部署集群。

智源平台集群部署分为两种场景：

- 智源平台单机扩展至集群：用户之前已经成功部署单台智源平台，为缓解单台的数据量压力，需要再部署多台智源平台扩展至集群。
- 直接部署智源平台集群：直接部署多台智源平台，并且组成集群。



注意:

- 部署智源平台集群时，第一台部署的智源平台作为主设备HA Master，第二、三台部署的智源平台作为Master，第四、五台部署的智源平台作为Slave。
- 如果用户之前已经成功部署两台或以上智源平台，在扩展至集群时，只有一台智源平台可以作为HA Master并确保该设备已部署智源平台系统，其他智源平台须先使用reset命令恢复出厂设置后加入集群。

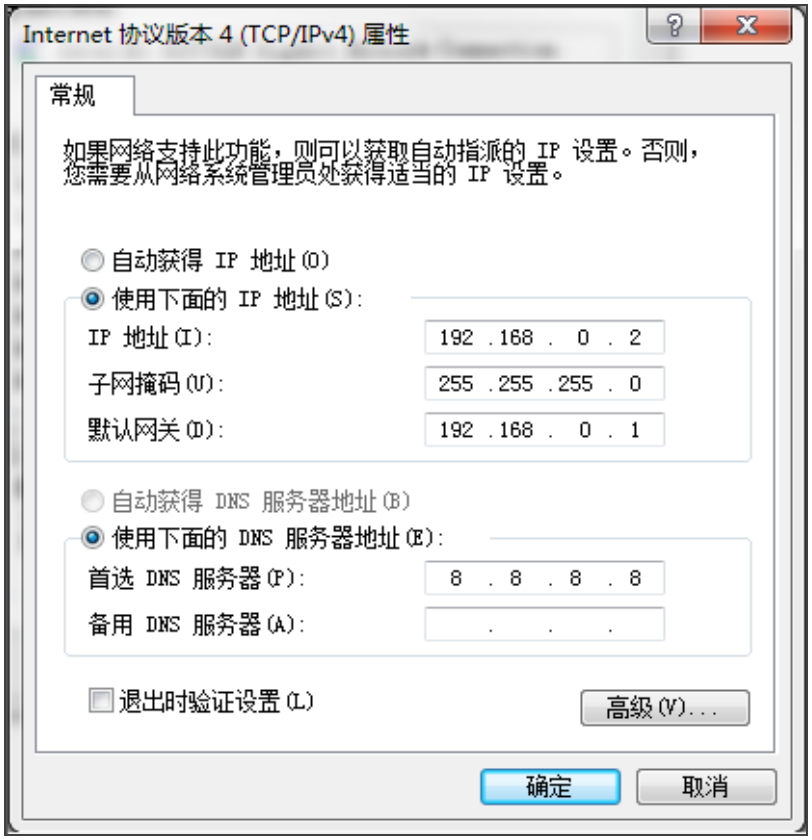
智源平台单机扩展至集群

根据上述组网图，用户之前已经成功部署单台智源平台，现需要将该设备作为HA Master，同时需要再部署3台智源平台扩展至集群。

部署智源平台Master

部署智源平台Master，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、使用SSH方式、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

6. 为eth0接口配置IP地址，输入以下命令：

   ```
   SG-6000#network ipconfig --interface eth0 --ip 10.180.0.5/24
   ```

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

7. 输入**show network ipconfig**命令检查当前接口配置。

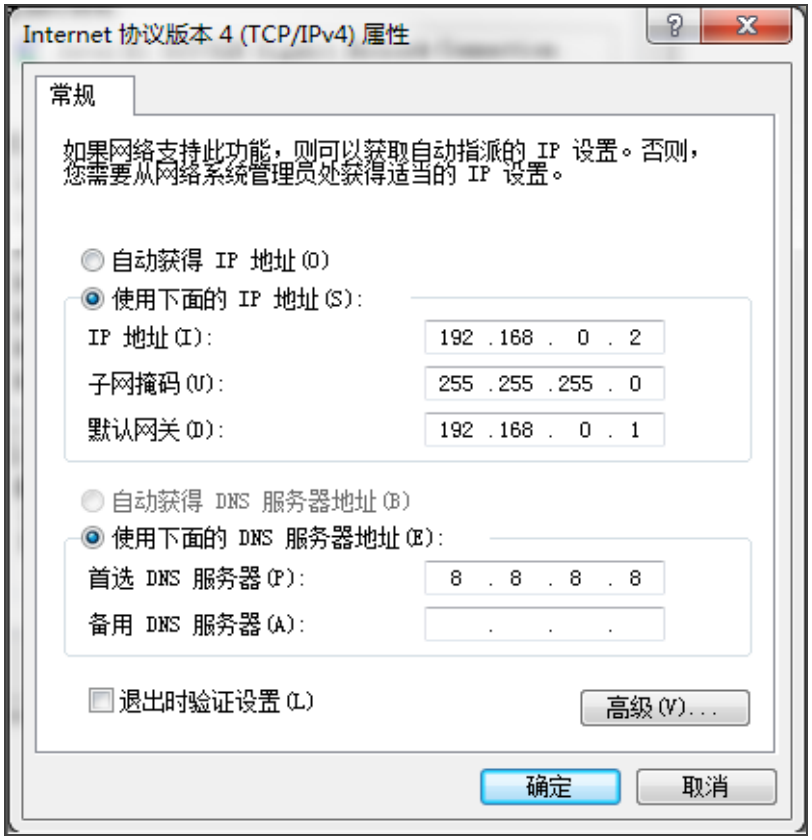
8. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

   ```
   SG-6000#cluster master --ip 10.180.0.4
   ```

部署智源平台Master

部署智源平台Master，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、使用SSH方式、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

6. 为eth0接口配置IP地址，输入以下命令：

```
SG-6000#network ipconfig --interface eth0 --ip 10.180.0.6/24
```

（如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

7. 输入**show network ipconfig**命令检查当前接口配置。

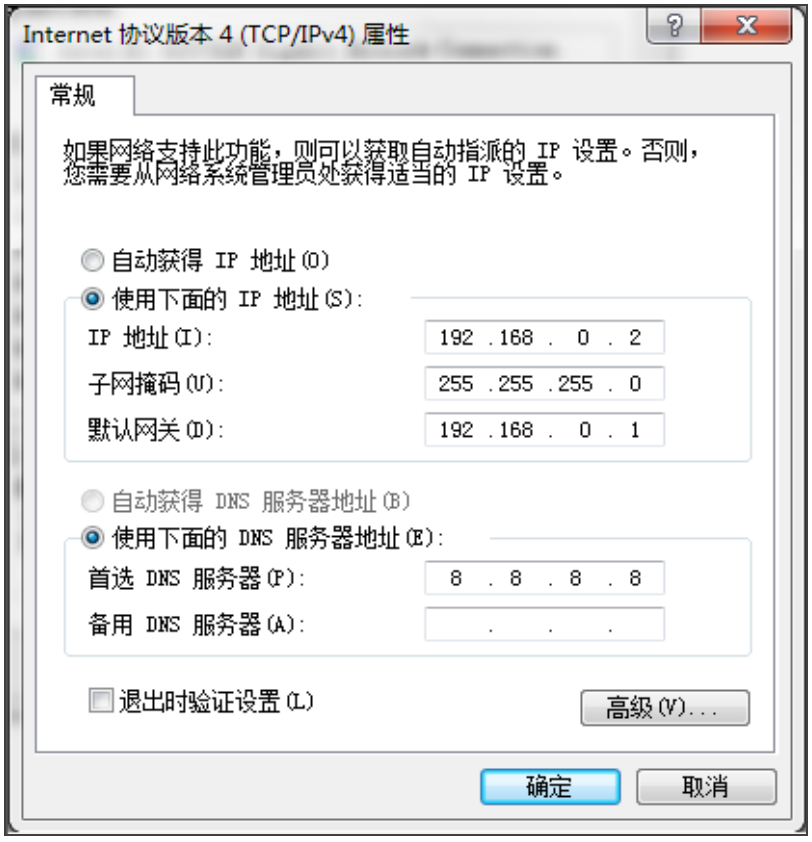
8. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

```
SG-6000# cluster master --ip 10.180.0.4
```

部署智源平台Slave

部署智源平台Slave，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、使用SSH方式、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

6. 为eth0接口配置IP地址，输入以下命令：

   ```
   SG-6000#network ipconfig --interface eth0 --ip 10.180.0.7/24
   ```

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

7. 输入**show network ipconfig**命令检查当前接口配置。

8. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

   ```
   SG-6000#cluster master --ip 10.180.0.4
   ```

将已部署的智源平台Master、Slave添加到集群

将已部署的智源平台Master、Slave添加到集群，按照以下步骤进行操作：

1. 在PC上运行终端仿真程序，并配置设备IP地址为“10.180.0.4”、使用SSH方式、用户名为“hillstone”，之后与设备建立连接。

2. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

3. 输入**network ha ipconfig**命令配置智源平台集群的虚拟IP地址（VIP），该VIP地址用于对外提供服务，输入以下命令：

   ```
   SG-6000#network ha ipconfig --ip 10.180.0.10
   Config network ha ip success
   ```

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#network ha ipv6 config --ipv6 X:X:X:X::X）

   注意：请确保该VIP地址与交换机在同一个网段。

4. 输入**cluster add node**命令分别指定各智源平台Master、Slave的地址，将所有智源平台Master、Slave加入集群中。

   添加Master：

   ```
   SG-6000# cluster add node --ip 10.180.0.5
   Start to add 10.180.0.5 to cluster...
   Generating and dispatching configuration for node .... success
   ```

```
Checking node2.hillstone is registered....
node2.hillstone registration .... success
Install system service on node2.hillstone .... success
Restart system service .... success
Scaling micro service platform .... success
add node successfully
```

添加Master：

```
SG-6000#cluster add node --ip 10.180.0.6
Start to add 10.180.0.6 to cluster...
Generating and dispatching configuration for node .... success
Checking node3.hillstone is registered....
node3.hillstone registration .... success
Install system service on node3.hillstone .... success
Restart system service .... success
Scaling micro service platform .... success
add node successfully
```

添加Slave：

```
SG-6000#cluster add node --ip 10.180.0.7
Start to add 10.180.0.7 to cluster...
Generating and dispatching configuration for node .... success
Checking node4.hillstone is registered....
node4.hillstone registration .... success
Install system service on node4.hillstone .... success
Restart system service .... success
Scaling micro service platform .... success
add node successfully
```

5. 提示成功后，完成智源平台集群的部署。智源平台集群即可通过VIP地址对外提供服务。

6. 输入**show network ha ipconfig**命令查看智源平台集群的VIP信息。

```
SG-6000#show network ha ipconfig
==========================================
```

```
manager vip internal vip
-------------------------------------------------------
10.180.0.10 192.168.53.222
-------------------------------------------------------
```

7. 输入**show cluster**命令查看智源平台集群概要信息，包括集群运行状态、各个智源平台详细信息等。

```
SG-6000#show cluster
=============================================================================-
=======
role ip sn status cpu(%) memory(%) disk(%) version
-------------------------------------------------------------------------------------------------------
ha master 10.180.0.4 419135059 active 25.5% 23.4% 0.3% V2.0R3
master 10.180.0.5 419135060 active 19.0% 19.2% 0.3% V2.0R3
master 10.180.0.6 419135061 active 20.9% 20.1% 0.3% V2.0R3
slave 10.180.0.7 419135062 active 22.8% 24.2% 0.3% V2.0R3
-------------------------------------------------------------------------------------------------------
```

8. 部署完成后，打开Web浏览器，在地址栏中输入https://10.180.0.10（即VIP地址）并按回车键。

9. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。

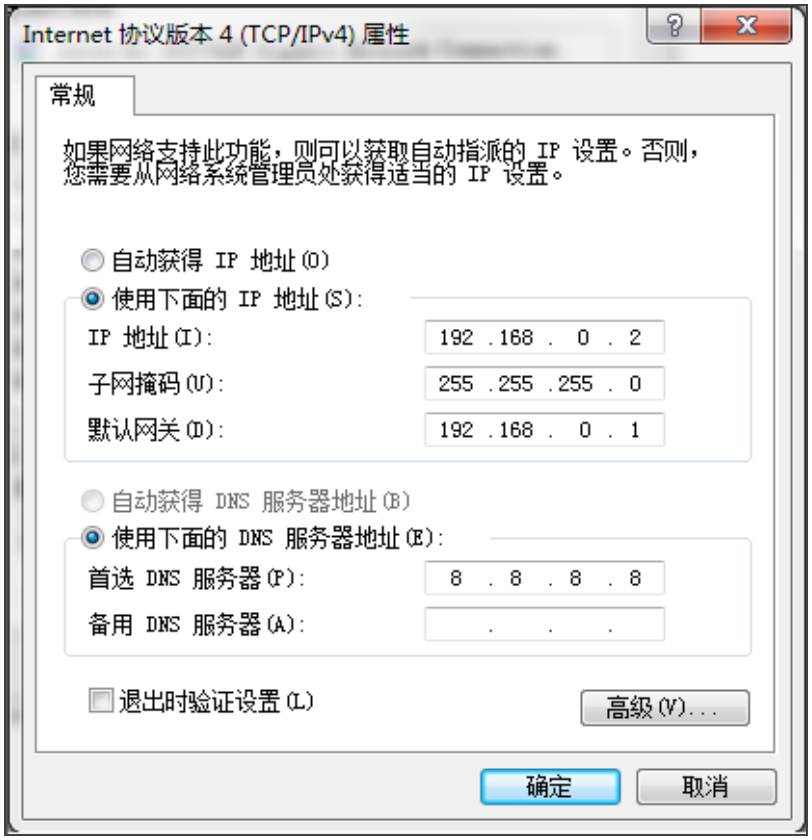
直接部署智源平台集群

根据上述组网图，直接部署4台智源平台，并且组成智源平台集群。

配置智源平台HA Master外部IP地址并部署系统

配置智源平台HA Master外部IP地址并部署系统，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、SSH版本为“SSH2”、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network internal segment**命令检查系统内部IP地址是否和用户网络中的IP地址冲突。如果不冲突，保持当前系统内部IP地址；如果冲突，输入**network internal segment --ip** *subnet/mask* 命令配置网段（掩码必须小于24，例如192.168.82.0/23），系统将会自动分配内部IP地址。

   注意：请确保该步骤在部署智源平台系统之前进行。在系统部署完成后，请尽量不要修改当前系统的内部IP地址。

6. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

7. 为eth0接口配置IP地址，输入以下命令：

   SG-6000#**network ipconfig --interface** eth0 **--ip** 10.180.0.4/24

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

8. 配置默认网关，输入以下命令：

   SG-6000#**network routeconfig --dst** 0.0.0.0/0 **--gateway** 10.180.0.1

   （如使用IPv6类型的IP地址，配置默认网关可使用SG-6000#**network routev6config --dst** *::/0* **--gateway** *X:X:X:X::X*）

9. （可选）如果有多网段管理需求，则为另一个link状态为true的接口配置IP地址，方法同步骤7。

   注意：智源平台只能存在一个默认网关，因此为了使多网段网络均能正常通信，应根据实际网络拓扑和需求配置相应的路由，方法同步骤8。

10. 输入**show network ipconfig**和**show network routeconfig**命令检查当前接口和路由配置。

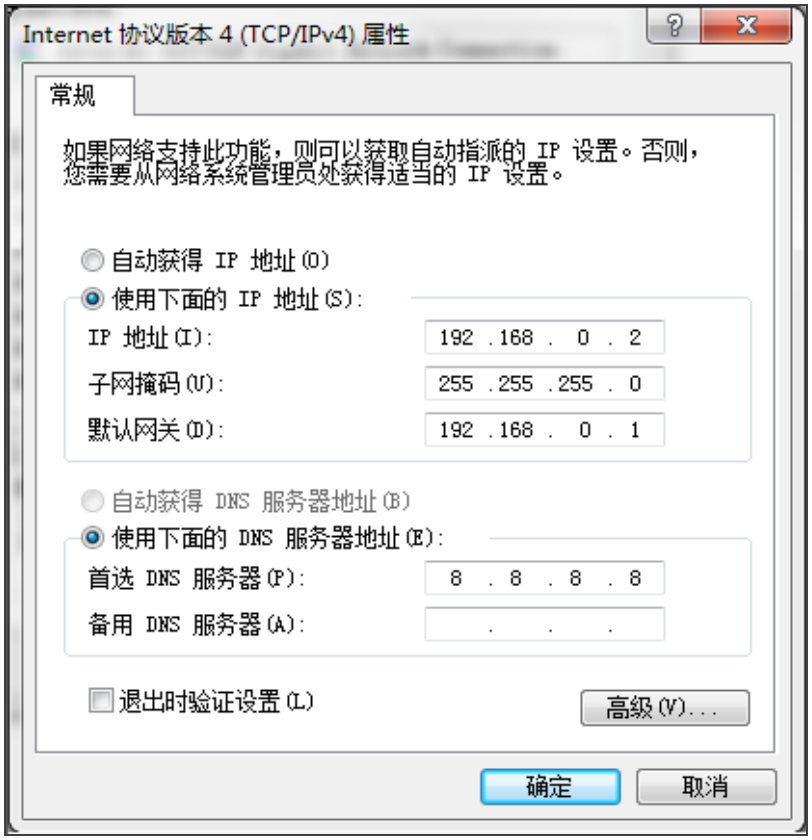
11. 输入**deploy standalone**命令并选择系统语言部署智源平台系统。

    注意：系统语言选定后如需修改，请reset设备并重新部署智源平台系统。

部署智源平台Master

部署智源平台Master，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、SSH版本为“SSH2”、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

6. 为eth0接口配置IP地址，输入以下命令：

   ```
   SG-6000#network ipconfig --interface eth0 --ip 10.180.0.5/24
   ```

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

7. 输入**show network ipconfig**命令检查当前接口配置。

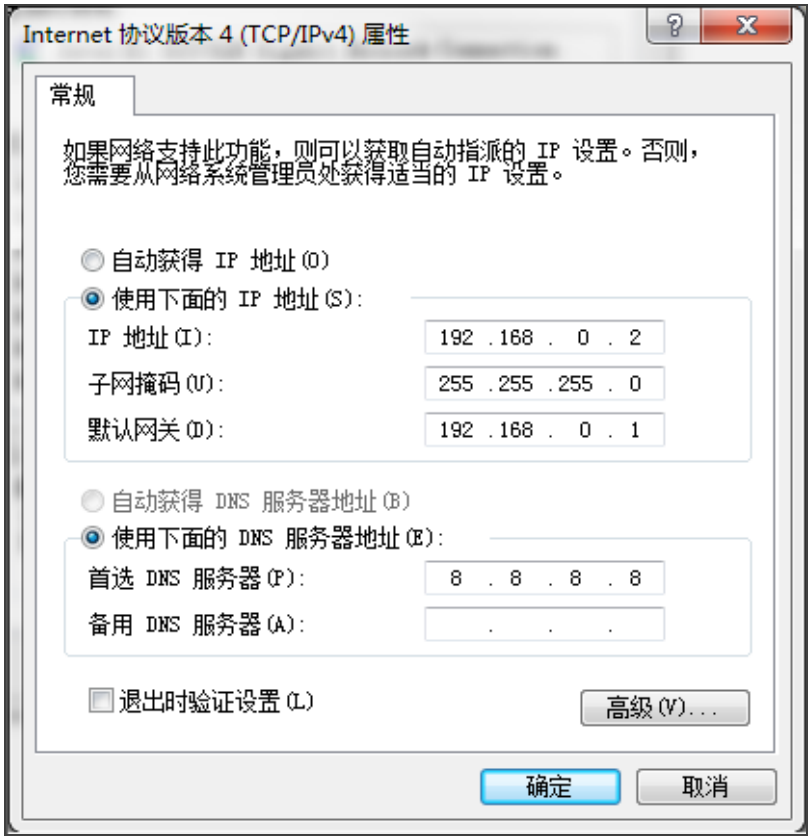
8. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

   ```
   SG-6000# cluster master --ip 10.180.0.4
   ```

部署智源平台Master

部署智源平台Master，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、SSH版本为“SSH2”、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

6. 为eth0接口配置IP地址，输入以下命令：

```
SG-6000#network ipconfig --interface eth0 --ip 10.180.0.6/24
```

（如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

7. 输入**show network ipconfig**命令检查当前接口配置。

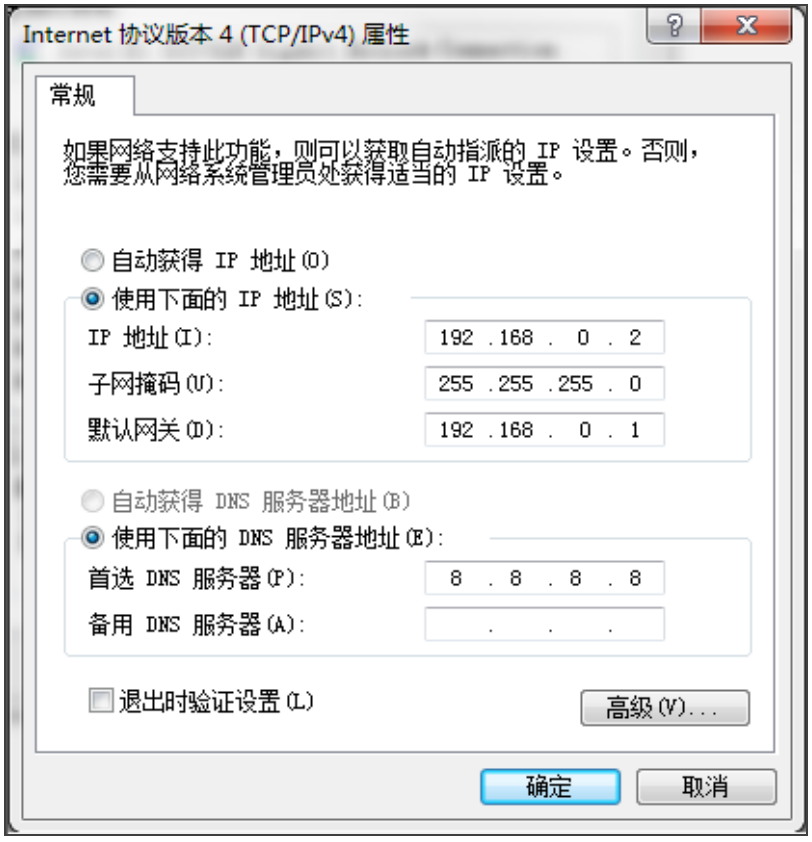
8. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

```
SG-6000# cluster master --ip 10.180.0.4
```

部署智源平台Slave

部署智源平台Slave，按照以下步骤进行操作：

1. 将PC的IP地址设置为与192.168.0.1/24同网段的IP地址，在PC的本地连接属性中，设置Internet协议版本4（TCP/IPv4）如下：



2. 用网线将PC与设备的eth0接口进行连接。

3. 在PC上运行终端仿真程序，并配置设备IP地址为“192.168.0.1”、SSH版本为“SSH2”、用户名为“hillstone”，之后与设备建立连接。

4. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

5. 输入**show network ipconfig**命令查看link状态为true的接口（link状态为true表示该接口已插入网线，本示例为eth0接口状态为true）。

6. 为eth0接口配置IP地址，输入以下命令：

   SG-6000#**network ipconfig --interface** eth0 **--ip** 10.180.0.7/24

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

7. 输入**show network ipconfig**命令检查当前接口配置。

8. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

   SG-6000# cluster master --ip 10.180.0.4

将已部署的智源平台Master、Slave添加到集群

将已部署的智源平台Master、Slave添加到集群，按照以下步骤进行操作：

1. 在PC上运行终端仿真程序，并配置设备IP地址为“10.180.0.4”、SSH版本为“SSH2”、用户名为“hillstone”，之后与设备建立连接。

2. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

3. 输入**network ha ipconfig**命令配置智源平台集群的虚拟IP地址（VIP），该VIP地址用于对外提供服务，输入以下命令：

   SG-6000#network ha ipconfig --ip 10.180.0.10

   Config network ha ip success

   （如智源平台为IPv6类型的IP地址，可使用SG-6000#network ha ipv6 config --ipv6 X:X:X:X::X）

   注意：请确保该VIP地址与交换机在同一个网段。

4. 输入**cluster add node**命令分别指定各智源平台Master、Slave的地址，将所有智源平台Master、Slave加入集群中。

   添加Master：

   SG-6000# cluster add node --ip 10.180.0.5

   Start to add 10.180.0.5 to cluster...

   Generating and dispatching configuration for node .... success

```
Checking node2.hillstone is registered....
node2.hillstone registration .... success
Install system service on node2.hillstone .... success
Restart system service .... success
Scaling micro service platform .... success
add node successfully
```

添加Master：

```
SG-6000#cluster add node --ip 10.180.0.6
Start to add 10.180.0.6 to cluster...
Generating and dispatching configuration for node .... success
Checking node3.hillstone is registered....
node3.hillstone registration .... success
Install system service on node3.hillstone .... success
Restart system service .... success
Scaling micro service platform .... success
add node successfully
```

添加Slave：

```
SG-6000#cluster add node --ip 10.180.0.7
Start to add 10.180.0.7 to cluster...
Generating and dispatching configuration for node .... success
Checking node4.hillstone is registered....
node4.hillstone registration .... success
Install system service on node4.hillstone .... success
Restart system service .... success
Scaling micro service platform .... success
add node successfully
```

5. 提示成功后，完成智源平台集群的部署。智源平台集群即可通过VIP地址对外提供服务。

6. 输入**show network ha ipconfig**命令查看智源平台集群的VIP信息。

```
SG-6000# show network ha ipconfig
==========================================
```

```
manager vip internal vip
-------------------------------------------------------
10.180.0.10 192.168.53.222
-------------------------------------------------------
```

7. 输入**show cluster**命令查看智源平台集群概要信息，包括集群运行状态、各个智源平台详细信息等。

```
SG-6000# show cluster
=============================================================================-
=======
role ip sn status cpu(%) memory(%) disk(%) version
-------------------------------------------------------------------------------------------------------
ha master 10.180.0.4 419135059 active 25.5% 23.4% 0.3% V2.0R3
master 10.180.0.5 419135060 active 19.0% 19.2% 0.3% V2.0R3
master 10.180.0.6 419135061 active 20.9% 20.1% 0.3% V2.0R3
slave 10.180.0.7 419135062 active 22.8% 24.2% 0.3% V2.0R3
-------------------------------------------------------------------------------------------------------
```

8. 部署完成后，打开Web浏览器，在地址栏中输入https://10.180.0.10（即VIP地址）并按回车键。

9. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。



注意: 使用默认用户名和密码初次登录后，建议立即修改默认密码。

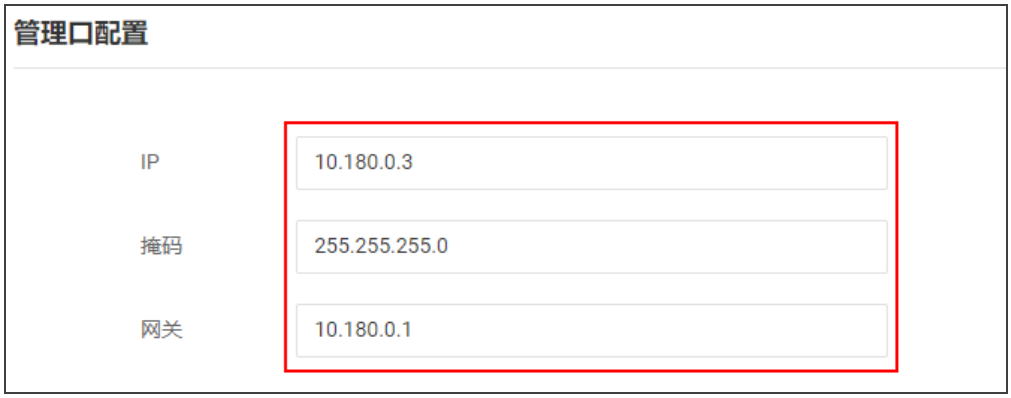
部署流量探针

流量探针采集网络设备的镜像流量，并将解析、分析、提取后的元数据（Meta Data）或者NetFlow信息发送至智源平台。

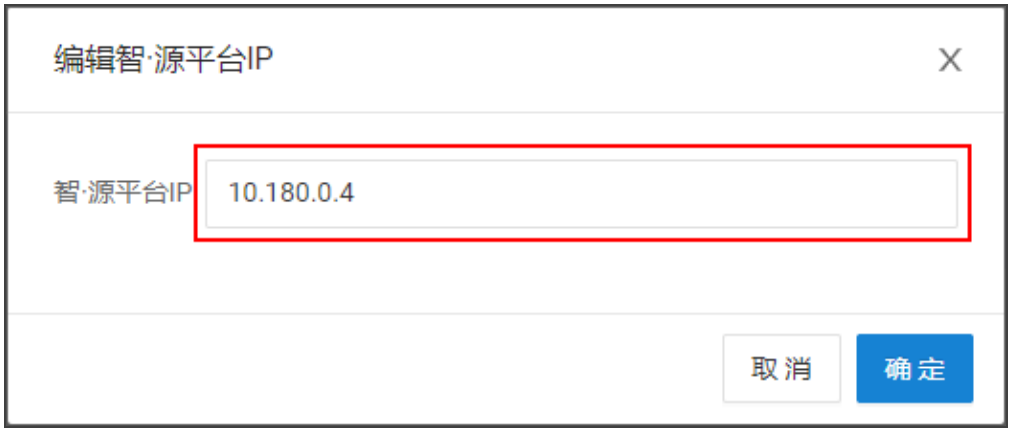
用户可根据需求选择是否部署流量探针。

部署流量探针，按照以下步骤进行操作：

1. 通过访问内网接口MGT接口的默认IP地址192.168.1.1/24，登录流量探针的WebUI管理界面。
2. 选择“系统设置 > 管理口配置”，配置MGT接口的IP地址与交换机在同一个网段。



3. 选择“系统状态 > 智源平台”，点击“编辑”按钮，配置智源平台的IP地址为10.180.0.4（单机部署时）或者配置为智源平台集群的VIP地址10.180.0.10。



4. 配置交换机，将流量镜像到流量探针的eth0/2接口上。流量探针处理镜像流量后，将其发送到智源平台。

5. （可选步骤）如需要将流量探针收到的镜像流量转发到其他设备，可以通过配置以下命令完成镜像流量转发功能：

   - 配置镜像流量转发：**mirror** *interface-name* **to** *interface-name*
   - 取消镜像流量转发配置：**no mirror** *interface-name* **to** *interface-name*
   - 查看流量探针各接口状态信息：**show interface**
   - 查看镜像流量转发配置信息：**show mirror**



注意:

- 镜像流量转发功能仅支持通过CLI方式配置。

部署威胁溯源插件

将威胁溯源插件安装部署在内网的用户主机上，即可采集终端的进程创建、网络访问、文件操作、注册表修改等相关行为信息，智源平台收集并展示采集到的用户主机系统的相关信息，从而实现威胁事件的溯源功能。

用户可根据需求选择是否部署威胁溯源插件。

部署环境要求

部署威胁溯源插件，对用户主机的环境要求，包括以下2个方面：

- 用户主机系统要求：
  - 使用Windows 7/ Windows server 2008 R2及以上版本
  - 内存要求1GB以上
  - 硬盘要求20GB以上
  - 具备以太网兼容网卡并支持TCP/IP协议
- 网络环境要求：确保用户主机与智源平台之间网络可达

部署方式

用户可以通过两种方式安装部署：

- "在用户主机上安装威胁溯源插件（单机安装方式）" 在第28页
- "在用户主机上安装威胁溯源插件（域安装方式）" 在第31页

在用户主机上安装威胁溯源插件（单机安装方式）

在用户主机上通过单机安装方式安装威胁溯源插件，即直接在用户主机上运行并安装msi格式的安装程序，主要包括以下几个方面内容：

- 准备工作
- 安装部署步骤
- 卸载威胁溯源插件
- 升级威胁溯源插件

准备工作

在安装威胁溯源插件之前，必须完成以下准备工作：

1. 获取智源平台的IP地址。
2. 通过山石网科销售人员下载获取对应系统的msi格式的安装程序压缩包（32位或64位）以及UpdateMsi工具压缩包。



注意: 请根据用户实际环境选择对应的插件安装程序，如64位系统选择64位的插件安装程序。

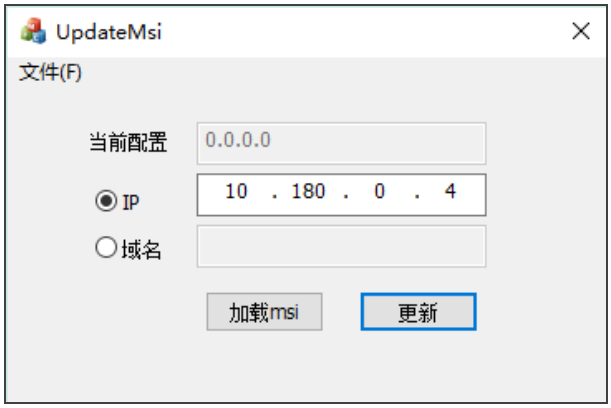
安装部署步骤

通过单机安装方式在用户主机上安装威胁溯源插件，请按照以下步骤进行操作：

步骤一：使用UpdateMsi工具更新安装程序

1. 解压缩获取到的msi格式的安装程序压缩包。
   安装程序包括：WinThreatTrace_x86.msi (32位)和WinThreatTrace_x64.msi（64位）。
2. 解压缩获取到的UpdateMsi工具压缩包。

3. 打开UpdateMsi工具，点击“加载msi”，加载成功后，输入智源平台的IP地址，点击“更新”。



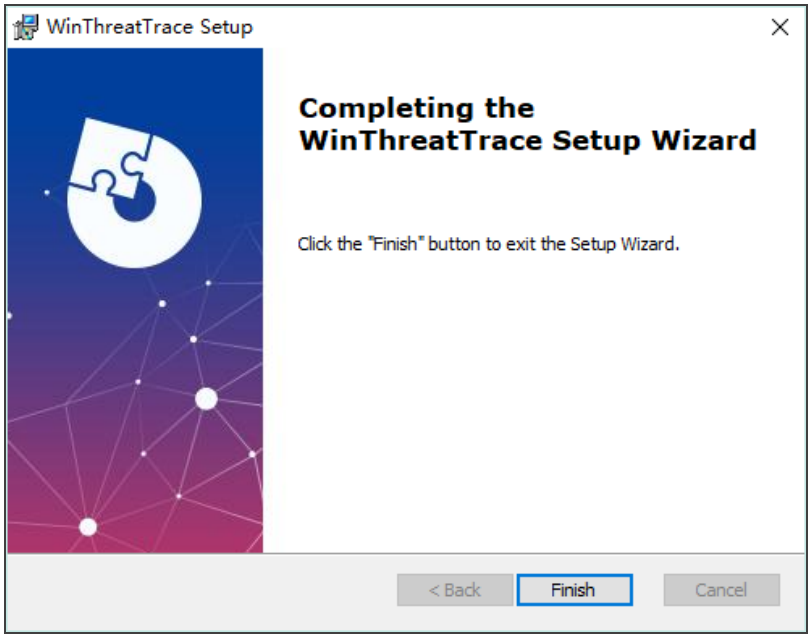
4. 提示“更新成功”后，即可。

步骤二：运行msi格式安装程序完成安装

1. 双击运行msi格式的安装程序。

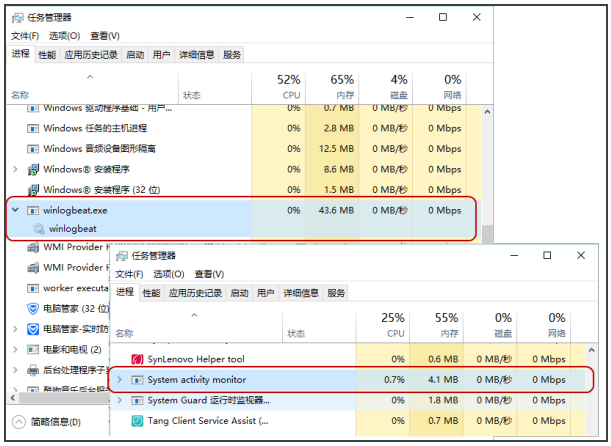
2. 根据提示，点击“next”按钮，然后确认安装位置后，点击“install”按钮，等待安装。

3. 点击“Finish”按钮，完成安装。



步骤三：确认进程

安装完成后，需要在任务管理器中确认System activity monitor和winlogbeat的进程。



卸载威胁溯源插件

如果需要在用户主机上卸载已经安装的威胁溯源插件，可以通过下面两种方式：

- 方式一：重新运行安装程序，根据提示点击“Remove”按钮，完成卸载。
- 方式二：进入Windows控制面板，选择“程序和功能”，在列表中选中已安装的“WinThreatTrace”，然后点击“卸载”，完成卸载。

升级威胁溯源插件

目前威胁溯源插件暂时不支持直接升级，如果需要升级插件，请先卸载已安装的威胁溯源插件，再使用最新的安装程序重新安装威胁溯源插件，从而完成插件升级。

在用户主机上安装威胁溯源插件（域安装方式）

在用户主机上通过域安装方式安装威胁溯源插件，即在域服务器中，通过下发组策略，向域用户推送安装威胁溯源插件。

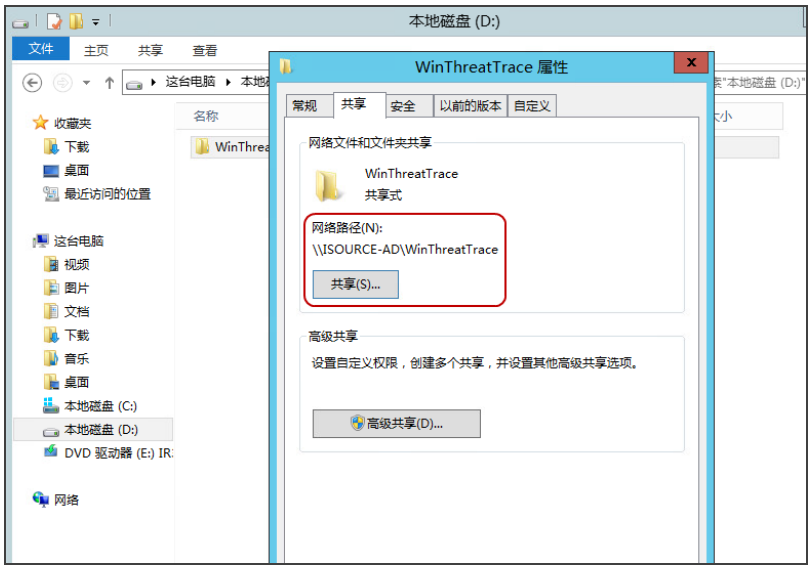
在用户主机上安装威胁溯源插件（域安装方式），主要包括以下几个方面内容：

- 准备工作
- 使用组策略分配安装威胁溯源插件
- 使用组策略卸载已分发安装的插件
- 使用组策略升级已分发安装的插件

准备工作

在通过域安装方式安装威胁溯源插件之前，必须完成以下准备工作：

1. 通过山石网科销售人员下载获取对应系统的msi格式的安装程序（32位或64位）。
2. 使用UpdateMsi工具更新安装程序（具体方法请参阅使用UpdateMsi工具更新安装程序）。
3. 在域服务器上创建一个共享文件夹，将安装程序存储到该共享文件夹中，并确保相应用户具有“读取”权限，以及确保域中的计算机能够访问该共享文件夹。



使用组策略分配安装威胁溯源插件

使用组策略分配安装威胁溯源插件，有两种方式：

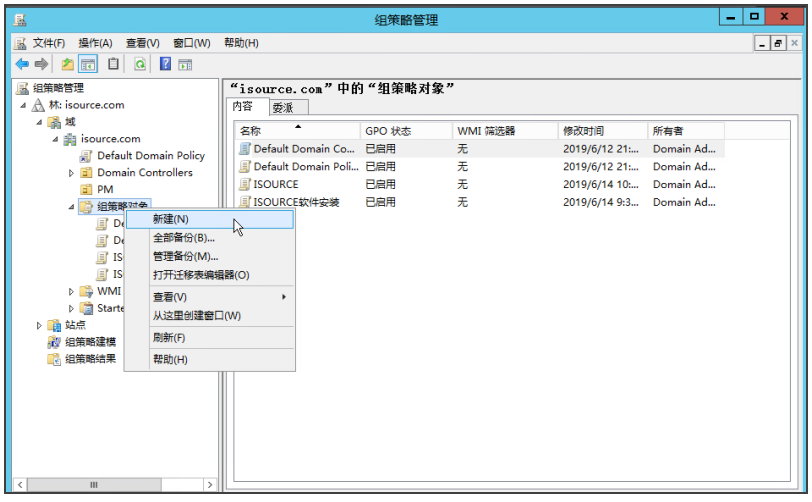
- 分配给域用户：当使用组策略将插件分配给域用户后，当域用户登录计算机时，计算机将会自动安装威胁溯源插件。
- 分配给域中的计算机：当使用组策略将插件分配给域中的计算机后，用户不用手动执行安装操作，当计算机重新启动时，将会自动安装威胁溯源插件。

分配给域用户

使用组策略将威胁溯源插件分配给域用户，请按照以下步骤进行操作：

步骤一：创建组策略对象

1. 在域服务器中，选择“开始 > 控制面板 > 系统和安全 > 管理工具”，双击“组策略管理”工具，打开<组策略管理>对话框。
2. 在左侧导航栏中依次展开节点，并右键点击“组策略对象”，选择“新建”，打开的<新建GPO>对话框。



3. 在<新建GPO>对话框中，输入组策略对象名称。



4. 点击“确定”，完成创建组策略对象。

步骤二：用户配置-编辑组策略部署软件

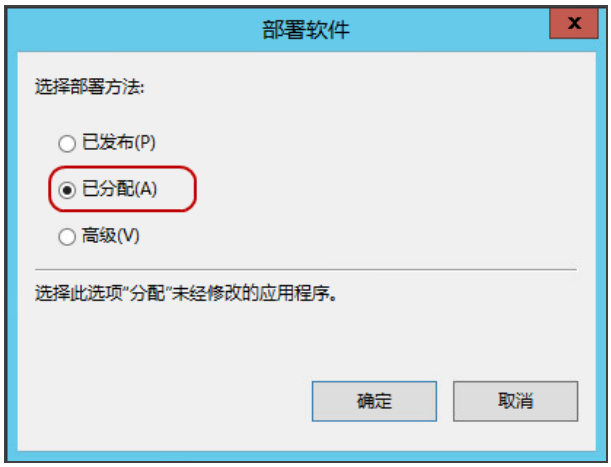
1. 右键点击已创建好的组策略对象，选择“编辑”，打开<组策略管理编辑器>对话框。

2. 在左侧导航栏选择“用户配置>策略>软件设置>软件安装”，右键点击“软件安装”，选择“新建>数据包”。

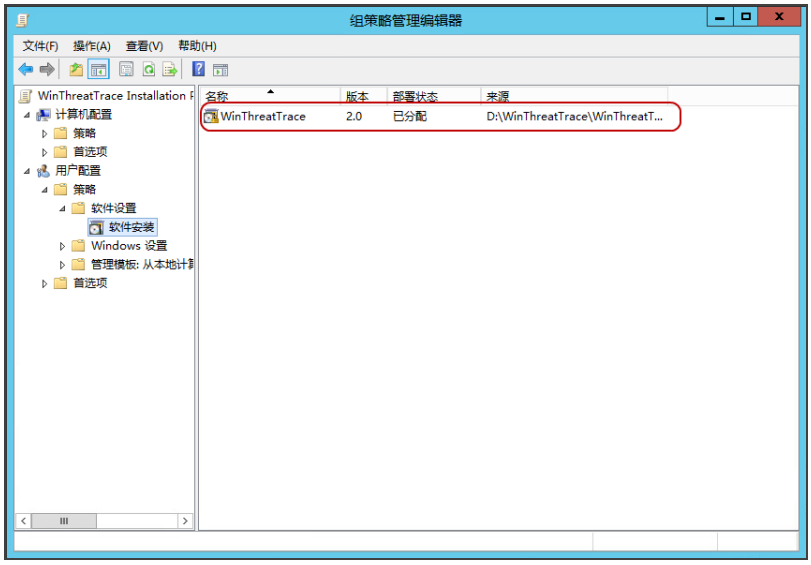


3. 选择已存储在共享文件夹中的威胁溯源插件安装程序。

4. 在弹出的<部署软件>对话框中，选择部署方式“已分配”，然后点击“确定”完成数据包的建立和部署。

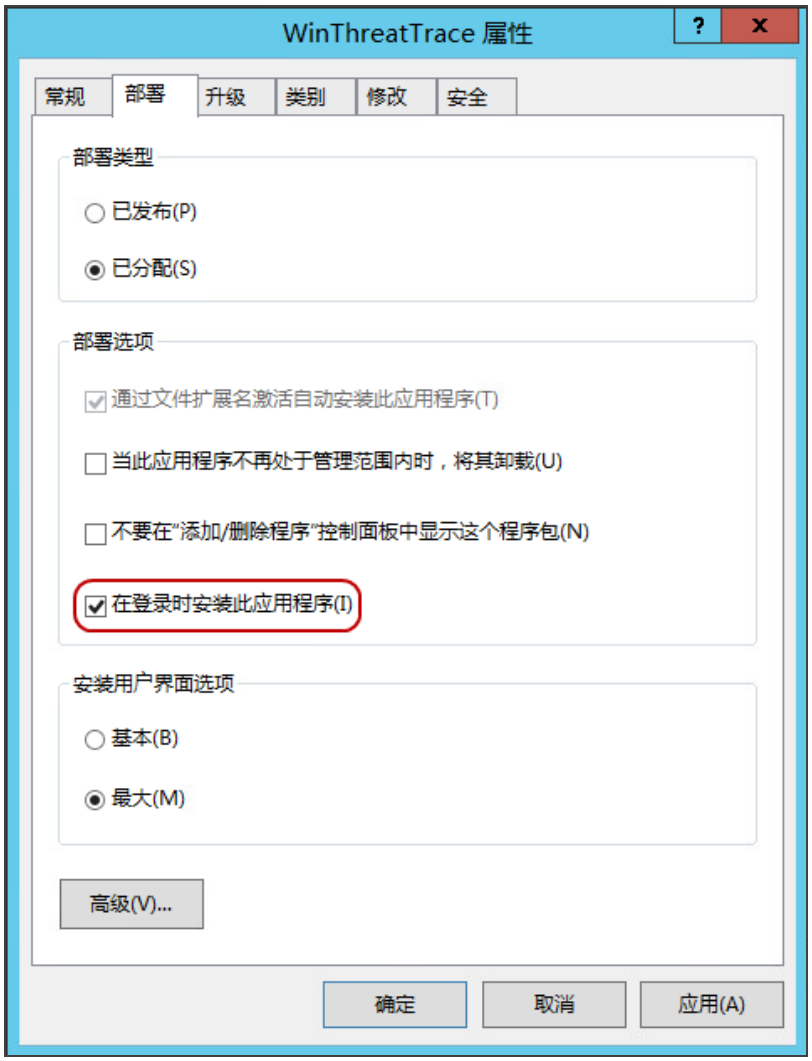


5. 完成数据包的建立后，即可显示在<组策略管理编辑器>对话框中。



6. 右键点击已部署的安装程序名称，选择“属性”。

7. 在属性对话框中，选择“部署”标签页，在“部署选项”部分，勾选“在登录时安装此应用程序”复选框。



8. 选择“安全”标签页，确保用户组具有“读取”权限。

9. 点击“确定”保存配置，返回到<组策略管理>对话框。

注意:

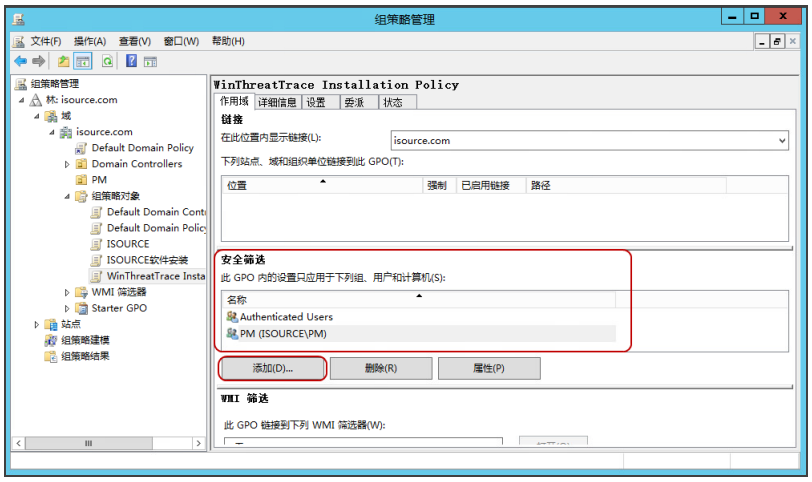
- 选择插件安装程序时，请使用共享文件夹的网络路径，否则将会无法读取文件。

- 请根据用户实际环境选择对应的插件安装程序，如64位系统选择64位的插件安装程序。

步骤三：将组策略应用到用户组织单位

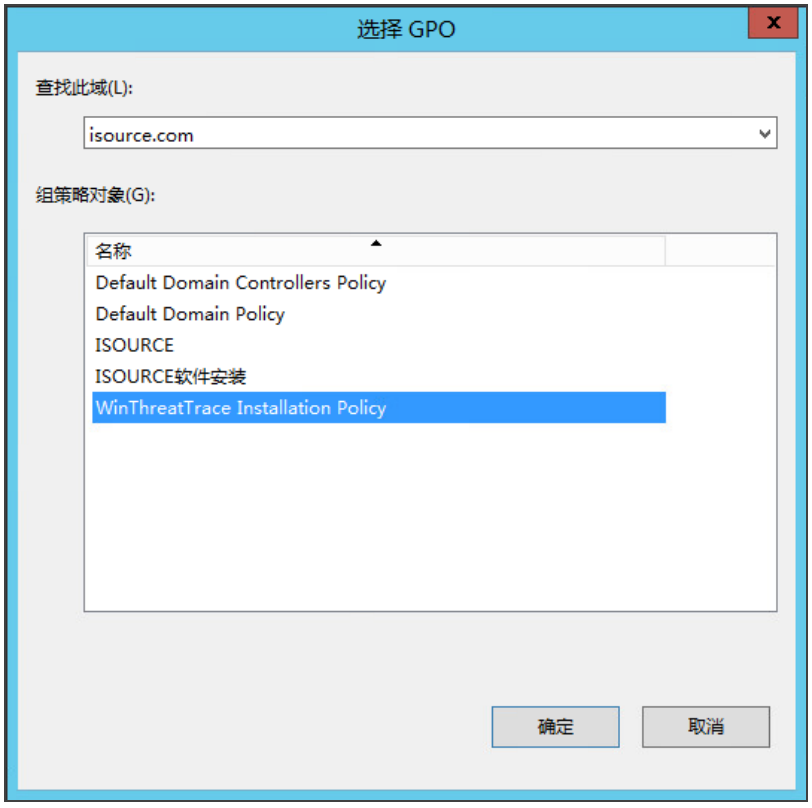
1. 在<组策略管理>对话框中，双击已创建的组策略名称。

2. 在“安全筛选”部分，点击“添加”按钮，添加需要安装威胁溯源插件的用户组。



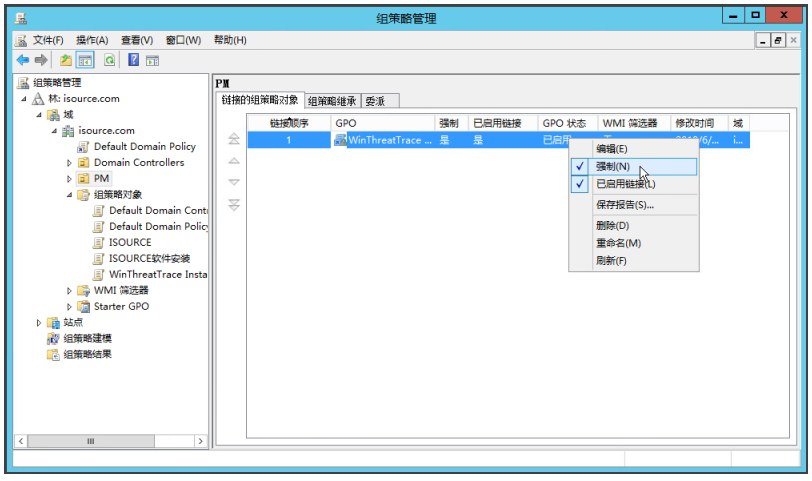
3. 在左侧导航栏中选择需要部署组策略的用户组织单位，右键点击用户组织单位名称，选择“链接现有GPO”，打开<选择GPO>对话框。

4. 在“组策略对象”部分，选择已创建的组策略对象名称。



5. 点击“确定”保存配置，并且返回到<组策略管理>对话框。

6. 为了保证该用户组织单位以及其子组织单位中可以强制执行该组策略，可以将该组策略指定为强制执行。 在“链接的组策略对象”标签页中，右键点击组策略名称，勾选“强制”。



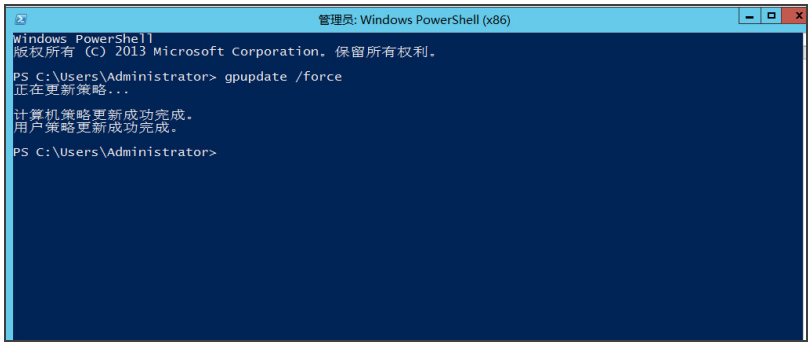


注意: 在链接组策略之前，需要保证用户组织单位已在域中创建完成。

步骤四：强制更新组策略

为了使得组策略生效，在完成上述步骤后，需要强制更新组策略。

1. 在域服务器上，选择“开始 > 控制面板 > 系统和安全 > 管理工具”，双击“Windows PowerShell”工具。
2. 在打开的命令窗口中输入“gpupdate /force”。



3. 提示更新完成后，关闭对话框即可。

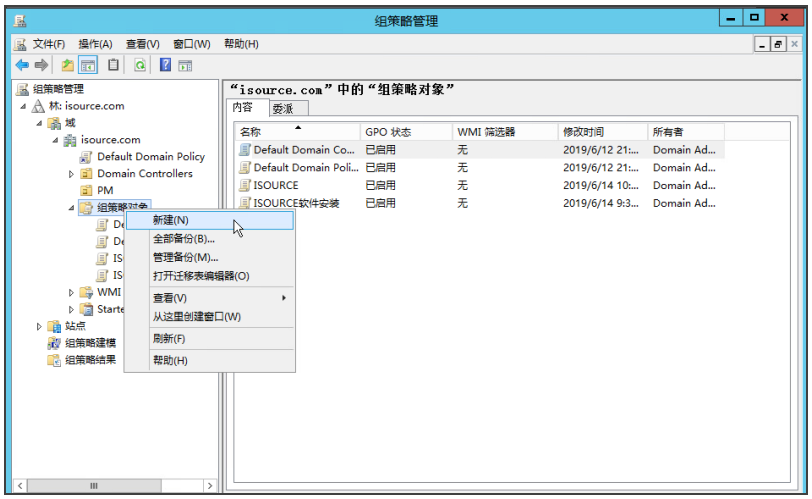
分配给域中的计算机

使用组策略将插件分配给域中的计算机，请按照以下步骤进行操作：

步骤一：创建组策略对象

1. 在域服务器上，选择“开始 > 控制面板 > 系统和安全 > 管理工具”，双击“组策略管理”工具，打开<组策略管理>对话框。

2. 在左侧导航栏中依次展开节点，并右键点击“组策略对象”，选择“新建”，打开的<新建GPO>对话框。



3. 在<新建GPO>对话框中，输入组策略对象名称。

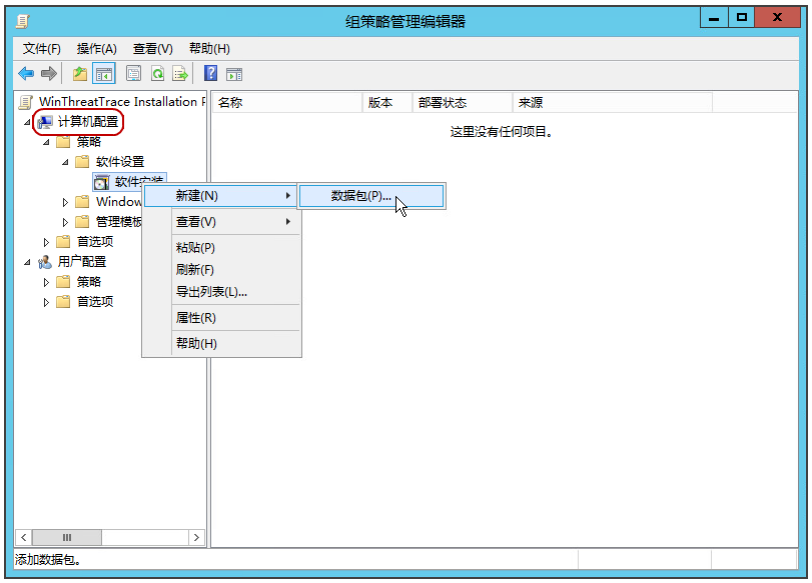


4. 点击“确定”，完成创建组策略对象。

步骤二：计算机配置-编辑组策略部署软件

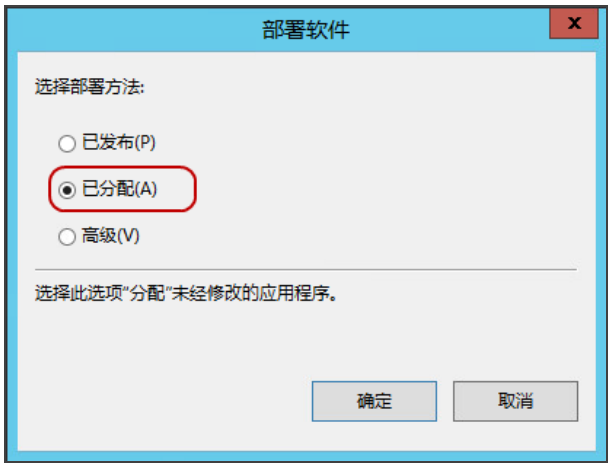
1. 右键点击已创建好的组策略对象，选择“编辑”，打开<组策略管理编辑器>对话框。

2. 在左侧导航栏选择“计算机配置>策略>软件设置>软件安装”，右键点击“软件安装”，选择“新建>数据包”。

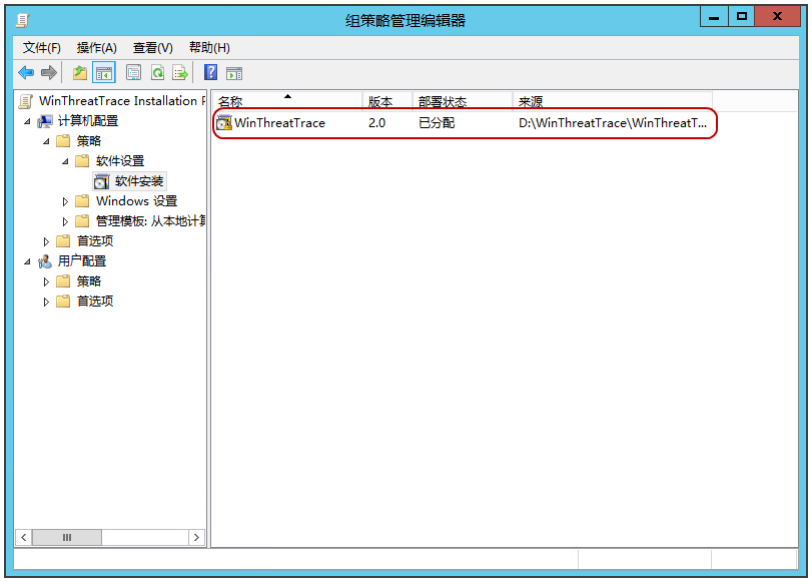


3. 选择已存储在共享文件夹中的威胁溯源插件安装程序。

4. 在弹出的<部署软件>对话框中，选择部署方式“已分配”，然后点击“确定”完成数据包的建立和部署。



5. 完成数据包的建立后，即可显示在<组策略管理编辑器>对话框中。



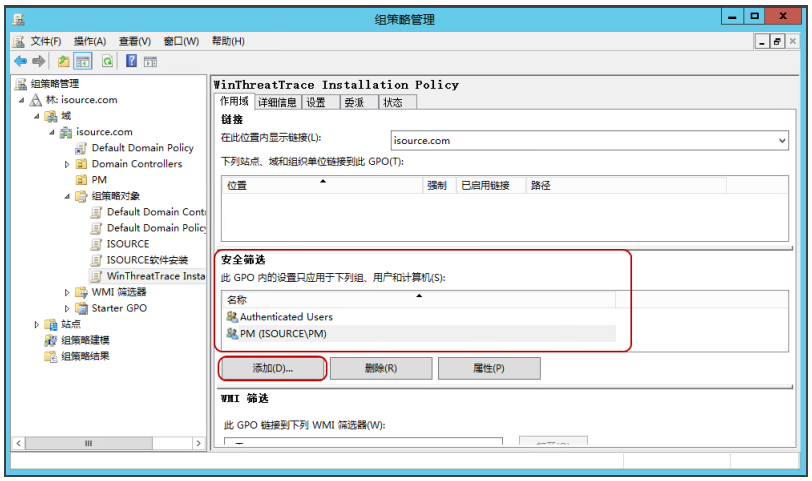
注意:

- 选择插件安装程序时，请使用共享文件夹的网络路径，否则将会无法读取文件。
- 请根据用户实际环境选择对应的插件安装程序，如64位系统选择64位的插件安装程序。

步骤三：将组策略应用到计算机组织单位

1. 在<组策略管理>对话框中，双击已创建的组策略名称。

2. 在“安全筛选”部分，点击“添加”按钮，添加需要安装威胁溯源插件的计算机组。

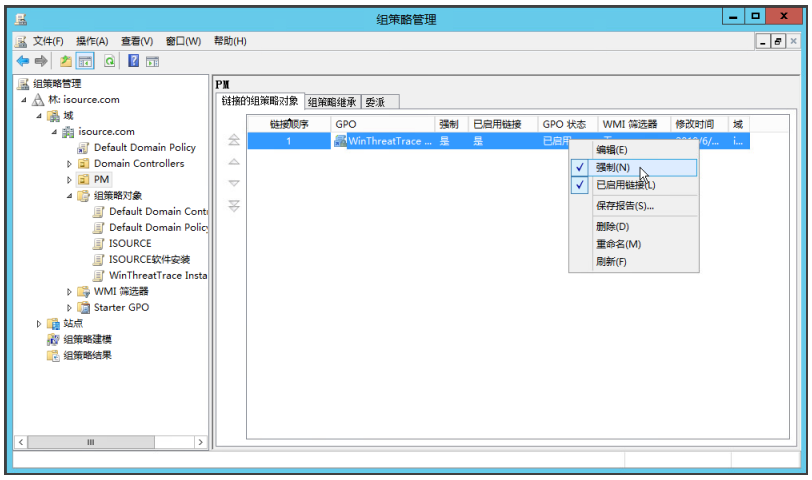


3. 在左侧导航栏中选择需要部署组策略的计算机组织单位，右键点击计算机组织单位名称，选择“链接现有GPO”，打开<选择GPO>对话框。

4. 在“组策略对象”部分，选择已创建的组策略对象名称。

5. 点击“确定”保存配置，并且返回到<组策略管理>对话框。

6. 为了保证该计算机组织单位以及其子组织单位中可以强制执行该组策略，可以将该组策略指定为强制执行。在“链接的组策略对象”标签页中，右键点击组策略名称，勾选“强制”。



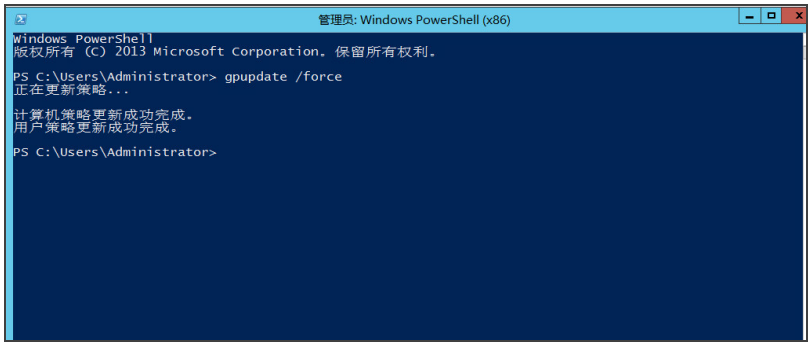


注意: 在链接组策略之前，需要保证计算机组织单位已在域中创建完成。

步骤四：强制更新组策略

为了使得组策略生效，在完成上述步骤后，需要强制更新组策略。

1. 在域服务器上，选择“开始 > 控制面板 > 系统和安全 > 管理工具”，双击“Windows PowerShell”工具。
2. 在打开的命令窗口中输入“gpupdate /force”。



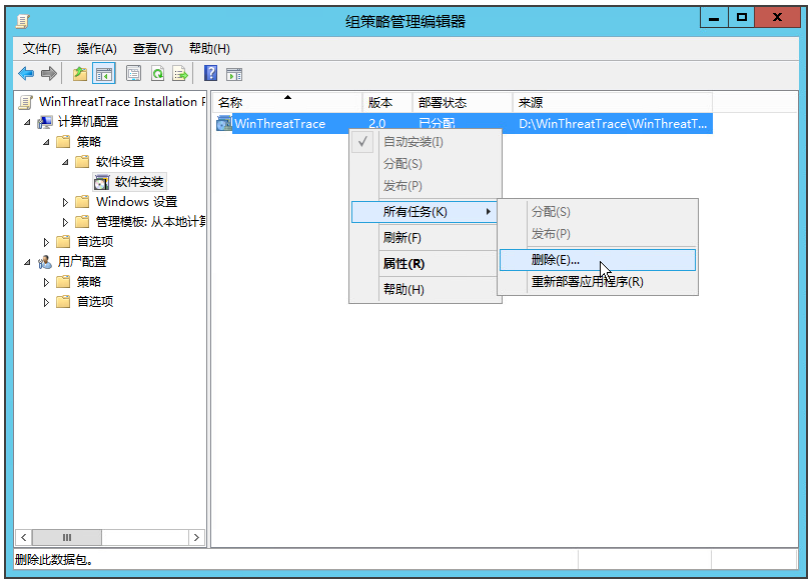
3. 提示更新完成后，关闭对话框即可。

使用组策略卸载已分发安装的插件

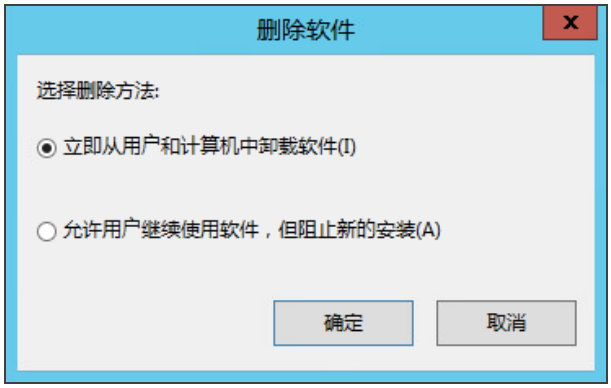
如果需要在使用组策略卸载已经分发安装的威胁溯源插件，请按照以下步骤进行操作：

1. 在域服务器上，选择“开始 > 控制面板 > 系统和安全 > 管理工具”，双击“组策略管理”工具，打开<组策略管理>对话框。
2. 在左侧导航栏中依次展开到“组策略对象”节点，右键点击指定的组策略对象名称，选择“编辑”，打开<组策略管理编辑器>对话框。
3. 在左侧导航栏选择“计算机配置（或用户配置）>策略>软件设置>软件安装”。

4. 在右侧的数据包记录中，右键点击软件名称，选择“所有任务>删除”，打开<删除软件>对话框。



5. 在<删除软件>对话框中，选择“立即从用户和计算机中卸载软件”。



完成上述步骤后，当匹配该组策略的计算机重启后，将会卸载已安装的威胁溯源插件。

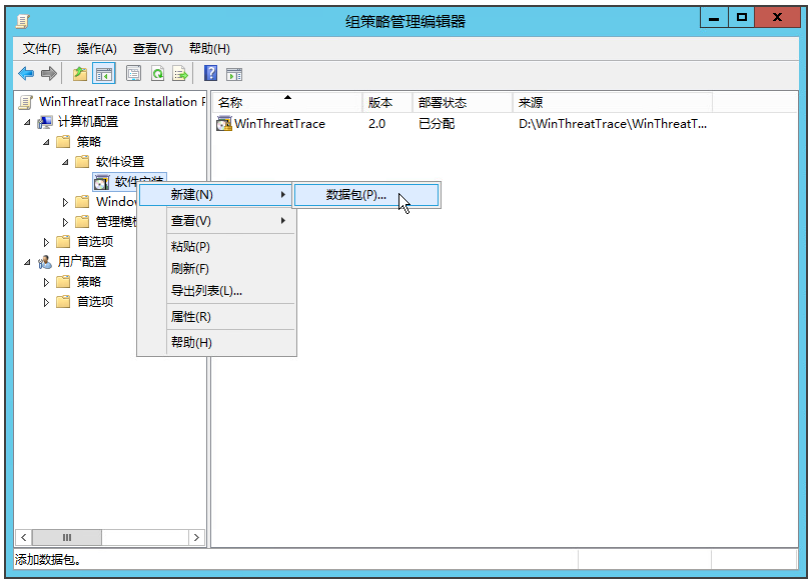
使用组策略升级已分发安装的插件

如果需要在使用组策略升级已经分发安装的威胁溯源插件（以分配给域中的计算机为例），请按照以下步骤进行操作：

1. 在域服务器上，选择“开始 > 控制面板 > 系统和安全 > 管理工具”，双击“组策略管理”工具，打开<组策略管理>对话框。

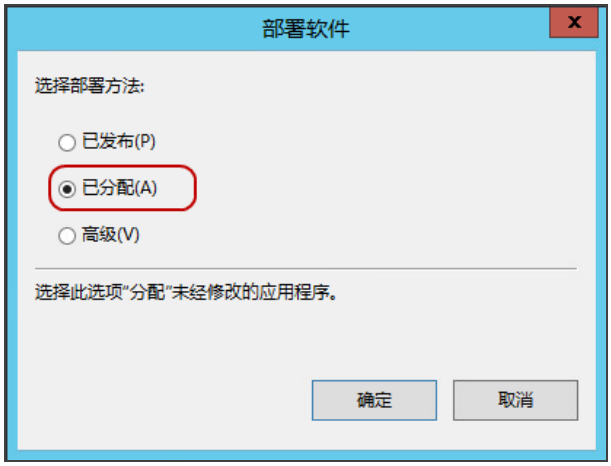
2. 在左侧导航栏中依次展开到“组策略对象”节点，右键点击指定的组策略对象名称，选择“编辑”，打开<组策略管理编辑器>对话框。

3. 在左侧导航栏选择“计算机配置>策略>软件设置>软件安装”，右键点击“软件安装”，选择“新建>数据包”。



4. 选择已存储在共享文件夹中的新版本威胁溯源插件安装程序。

5. 在弹出的<部署软件>对话框中，选择部署方式“已分配”，然后点击“确定”完成新版本数据包的建立和部署。



6. 完成新版本数据包建立后，执行强制更新组策略步骤，使得更新的组策略生效。（具体方法请参阅上述步骤四：强制更新组策略）

完成上述步骤后，当匹配该组策略的计算机重启后，威胁溯源插件即会更新成新版本。

部署威胁探针

目前，山石智 · 感-智能内网威胁感知系统（sBDS）设备或者威胁探针系列设备均可以作为威胁探针连接到智源平台，威胁探针设备对收到的镜像流量检测、监测以及分析后，再将产生的威胁信息发送至智源平台。

用户可根据需求选择是否部署威胁探针。

部署威胁探针，请按照以下配置步骤进行操作：

1. 通过访问内网接口MGT接口的默认IP地址192.168.1.1/24，登录威胁探针的WebUI管理界面。
2. 选择“配置管理>系统配置 > 连接智源”，进入配置智源参数页面。



3. 选中“连接智源”后的“启用”复选框，开启连接智源平台功能。
4. 在“服务器IP/域名”文本框输入智源平台的IP地址10.180.0.4（单机部署时）或者配置为智源平台集群的VIP地址10.180.0.10。
5. 在“服务器端口”文本框输入智源平台的连接端口号7777。
6. 点击“确定”按钮保存所做的配置。
7. 连接成功后，在“状态”后显示智源平台的状态：已连接。
8. 配置交换机，将流量镜像到威胁探针的eth0/2接口上。威胁探针检测、监测以及分析后，再将产生的威胁信息发送到智源平台。

注意: 当使用sBDS设备作为威胁探针时，为使功能生效， 请先确保已经完成如下配置步骤：

1. 开启威胁日志功能。

2. 指定将威胁日志输出到日志服务器。

3. 将日志服务器的主机名称配置为智源平台的IP地址/域名。

4. 在<日志服务器配置>中勾选“威胁日志” 作为日志服务器接收的日志类型。



关于sBDS设备的详细配置方法， 请参阅《山石智 · 感-智能内网威胁感知系统 WebUI 用户手册》。

部署山石云鉴

山石云鉴主机安全管理系统（CloudDis，简称山石云鉴），围绕主机检测、响应、预防可持续安全运营，实现主机安全全生命周期管理。通过对主机进行脆弱性检测、东西向微隔离管控、多锚点风险检测、多层级安全响应等措施，解决主机资产管理、安全加固、东西向流量防护、威胁实时检测、应急响应、失陷主机定位等安全问题，能够有效帮助安全管理人员应对日趋严峻的主机风险态势。

山石云鉴主机安全管理系统可以将资产信息、风险行为信息以Syslog日志的形式发送至智源平台。

用户可根据需求选择是否部署山石云鉴。

注意: 部署山石云鉴的详细步骤，可参考《山石云鉴主机安全管理系统部署手册》。

完成部署山石云鉴后，需配置“syslog参数配置”以及启用默认日志解析规则“山石云鉴Syslog日志解析规则”，以实现与智源平台的对接和发送相关信息。

山石云鉴的Syslog参数配置，请按照以下配置步骤进行操作：

1. 访问已部署好的山石云鉴主机安全管理系统，并登录系统。
2. 选择“系统配置>参数配置”，打开参数配置页面。



3. 在“syslog 参数配置”部分，勾选“启用Syslog”复选框，选择“UDP”单选按钮。
4. 在“IP/域名”文本框中输入智源平台的IP地址10.180.0.4（单机部署时）或者配置为智源平台集群的VIP地址10.180.0.10。
5. 在“端口”文本框输入智源平台的连接端口号514。

6. 点击按钮，打开<syslog详细配置>对话框，勾选“资产”和“风险行为”复选框，并指定上报频率。

7. 点击按钮，保存配置。

启用“山石云鉴Syslog日志解析规则”，请按照以下配置步骤进行操作：

1. 访问并登录已部署好的智源平台（10.180.0.4）。

2. 选择“日志管理>日志解析”，并点击<日志解析规则>标签页。

3. 在列表中“山石云鉴Syslog日志解析规则”的“状态”列中，点击启用按钮。

完成上述配置后，山石云鉴主机安全管理系统的资产信息、风险行为信息将会以Syslog日志的形式发送至智源平台。

软件化部署

山石网科的软件化智源，是一个纯软件形态的产品，是部署及运行在终端主机、虚拟机上的智源系统。

本节介绍如何将软件化智源部署到不同的环境中，包括VMware、Linux系统的终端主机以及Windows系统的终端主机。

适用场景

- 在ESXi Server主机上安装软件化智源，请参考“在VMware ESXi上部署软件化智源”。
- 在Linux系统的终端主机上安装软件化智源，请参考“在CentOS 7系统终端主机上部署软件化智源”。
- 在Windows系统的终端主机上安装软件化智源，请参考“在Windows 10系统终端主机上部署软件化智源”。

产品信息

软件化智源产品包含多种型号，用户可以根据实际需要来选择，每种型号的产品要求最低配置要求如下：

产品型号	最低配置要求
SG-6000-ISC6205	64位CPU，安装和运行时需要20个内核，128G内存
SG-6000-ISC6210	64位CPU，安装和运行时需要24个内核，128G内存
SG-6000-ISC6220	64位CPU，安装和运行时需要48个内核，256G内存

在VMware ESXi上部署软件化智源

软件化智源系统通过VMDK格式封装，可以安装在任意一台支持VMware ESXi 虚拟机的X86设备上。

在VMware ESXi服务器上部署软件化智源，要求您必须已经熟悉VMware的vSphere Hypervisor 架构、ESXi主机设置、VMware虚拟机部署等知识。

系统要求和限制

软件化智源的使用要求和限制：

- VMware ESXi 的版本为6.7。
- 虚拟机至少需要64位CPU、安装和运行时需要24个内核、128G内存，具体安装的产品型号规格，请参阅产品信息。

部署步骤

在安装软件化智源之前，请先设置好ESXi Server主机，并获取OVF+VMDK文件。

第一步：访问登录VMware ESXi 6.7平台

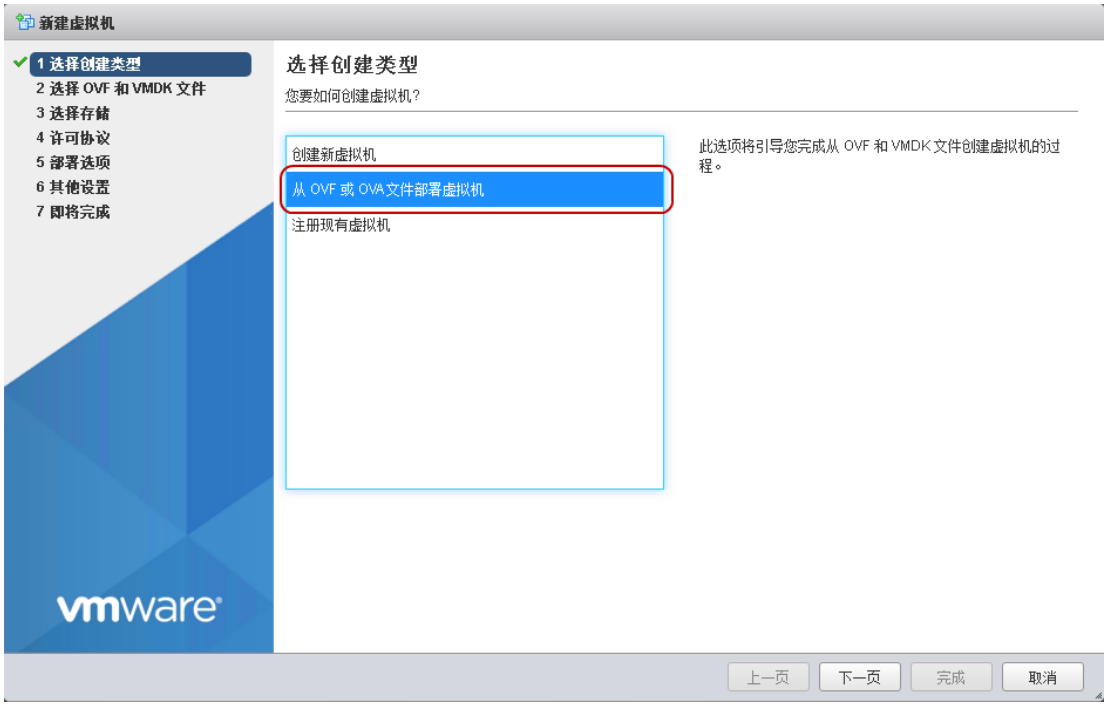
1. 将OVF+VMDK文件保存在本地。
2. 访问VMware ESXi 6.7平台，输入用户名和密码，点击“登录”。

第二步：创建虚拟机

1. 登录VMware ESXi 6.7平台后，点击左侧“虚拟机”节点，然后在右侧页面中点击“创建/注册虚拟机”。



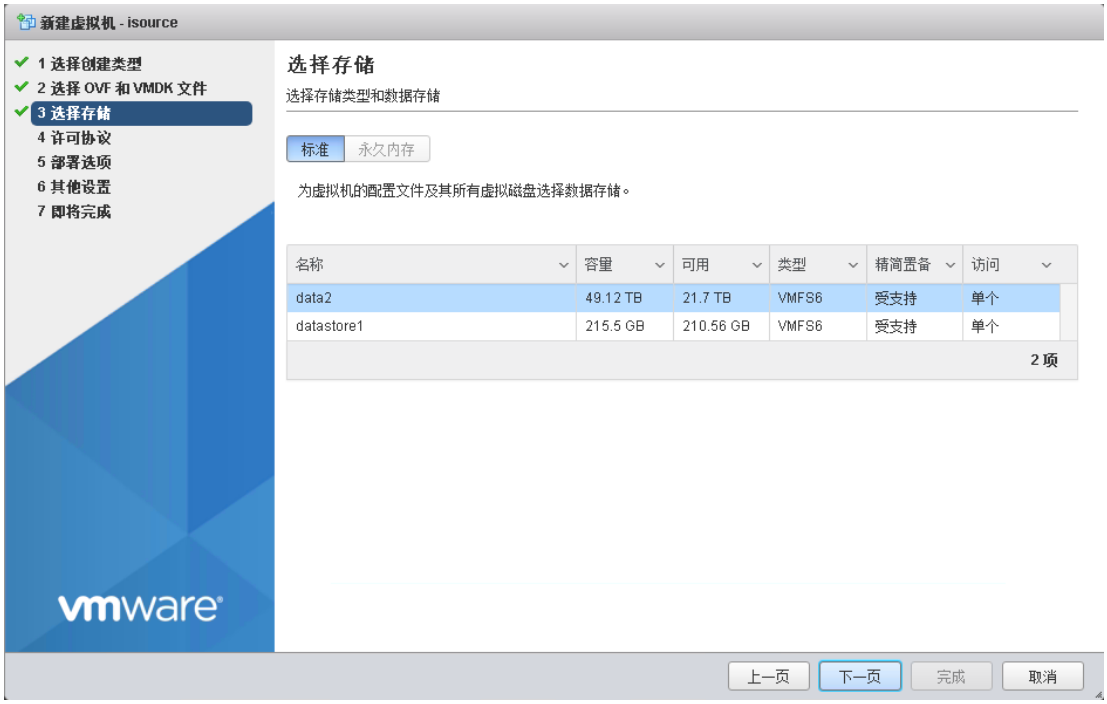
2. 选择创建的虚拟机类型。在<新建虚拟机>对话框中，点击“1 选择创建类型 > 从OVF文件部署虚拟机”，然后点击“下一页”。



3. 为要部署的虚拟机选择OVF+VMDK文件。输入虚拟机名称后，选择OVF+VMDK文件或直接将文件拖动至提示位置，然后点击“下一页”。



4. 选择存储类型和智源系统安装的硬盘位置，然后点击“下一页”。



注意：需选择大小在1TB以上的硬盘。

5. 配置部署选项，根据网络环境选择“网络映射”，“磁盘置备”处选择“精简”，然后点击“下一页”。

6. 检查配置后，点击“完成”按钮。可忽略报错提示。

7. 稍等片刻，待系统文件上载磁盘完成后，即可完成虚拟机创建。

第三步：配置智源访问地址以及部署系统

1. 在“虚拟机”列表中，点击已创建的虚拟机名称。

2. 点击“控制台>打开浏览器控制台”或者直接单击控制台缩略图，打开控制台页面。

3. 输入**`show network internal segment`**命令检查系统内部IP网段是否和用户网络中的IP地址冲突。如果不冲突，保持当前系统内部IP网段；如果冲突，输入**`network internal segment --ip`** *`subnet/mask`* 命令配置网段（掩码必须小于24，例如192.168.82.0/23），并在配置的网段中选择第一个IP地址作为该设备的内部IP地址。

   注意：请确保该步骤中配置的网段内的所有IP地址均不会和用户网络中的IP地址冲突，并且该步

骤需要在部署智源平台系统之前进行。在系统部署完成后，请尽量不要修改当前系统的内部IP地址。

4. 为宿主机接口（例如eth0）配置软件化智源的IP地址（例如10.180.0.4），输入以下命令：
   `SG-6000#network ipconfig --interface eth0 --ip 10.180.0.4/24`
   （如软件化智源为IPv6类型的IP地址，可使用`SG-6000#network ipv6config --interface eth0 --ipv6 X:X:X:X::X/ipv6-prefix`）。

5. 配置默认网关，输入以下命令：
   `SG-6000#network routeconfig --dst 0.0.0.0/0 --gateway 10.180.0.1`
   （如使用IPv6类型的IP地址，配置默认网关可使用`SG-6000#network routev6config --dst ::/0 --gateway X:X:X:X::X`）

6. （可选）如果有多网段管理需求，则为另一个接口配置IP地址，方法同步骤4。
   注意：软件化智源只能存在一个默认网关，因此为了使多网段网络均能正常通信，应根据实际网络拓扑和需求配置相应的路由，方法同步骤5。

7. 输入**deploy standalone**命令并选择系统语言部署智源系统。
   注意：系统语言选定后如需修改，请reset设备并重新部署智源系统。

第四步：访问智源系统

1. 打开Web浏览器，在地址栏中输入智源系统的IP地址（https://10.180.0.4）并按回车键。

2. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。



注意: 激活状态下的智源系统才能够正常使用，系统激活具体方式，请参阅激活智源系统。

在CentOS 7系统终端主机上部署软件化智源

软件化智源系统通过QCOW2格式封装，可以安装在任意一台Linux系统终端主机上。

在CentOS 7系统终端主机上部署软件化智源，要求您必须熟悉Libvirt和qemu-kvm环境的搭建方式。

系统要求和限制

软件化智源的使用要求和限制：

- Linux系统的版本为CentOS 7，且系统必须能够访问互联网。
- 至少需要64位CPU、安装和运行时需要24个内核、128G内存，具体安装的产品型号规格，请参阅产品信息。

准备工作

在安装软件化智源之前，请先完成Libvirt和qemu-kvm环境的搭建、网络配置、已安装远程终端控制软件（本示例以MobaXterm为例）以及已获取QCOW2格式系统文件。

CentOS 7系统环境下的网络配置，建议用户在部署前完成创建并配置网桥（Bridge），。具体步骤参考如下：

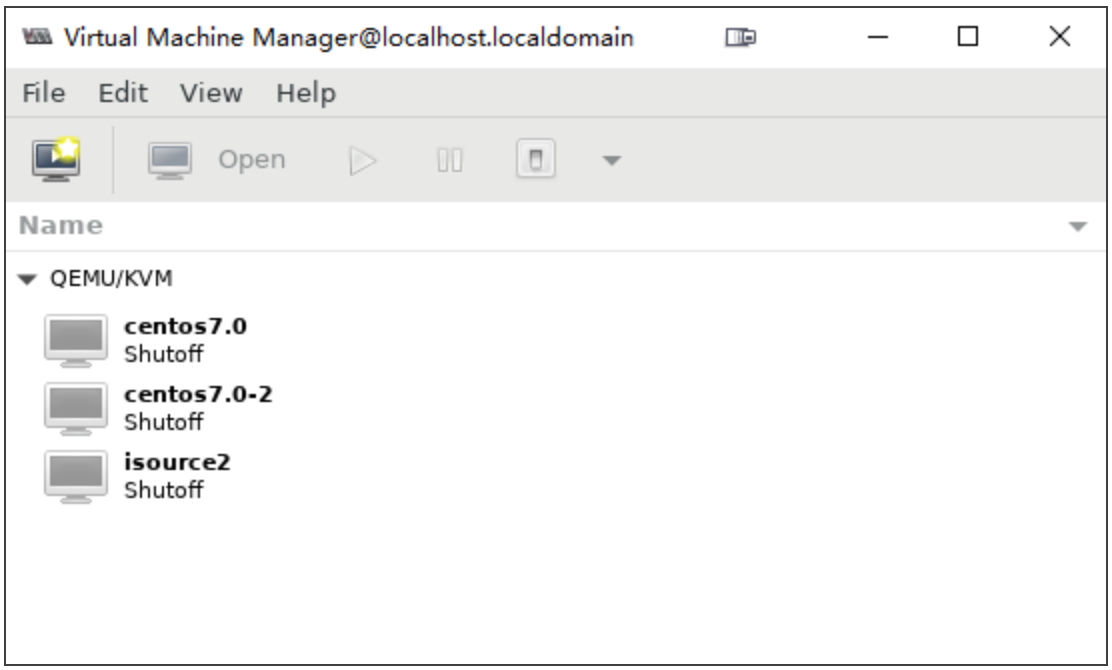
1. 安装网桥工具bridge-utils：输入命令**`yum install bridge-utils`**。
2. 创建网桥br0：输入命令**`brctl addbr br0`**。
3. 将eth0设置为网桥br0的接口，通过此方法将网桥与物理网卡绑定：输入命令**`brctl addif br0 eth0`**。
4. 重启网络： 输入命令**`systemctl restart network`**。

部署步骤

第一步：启用虚拟机管理图形化界面

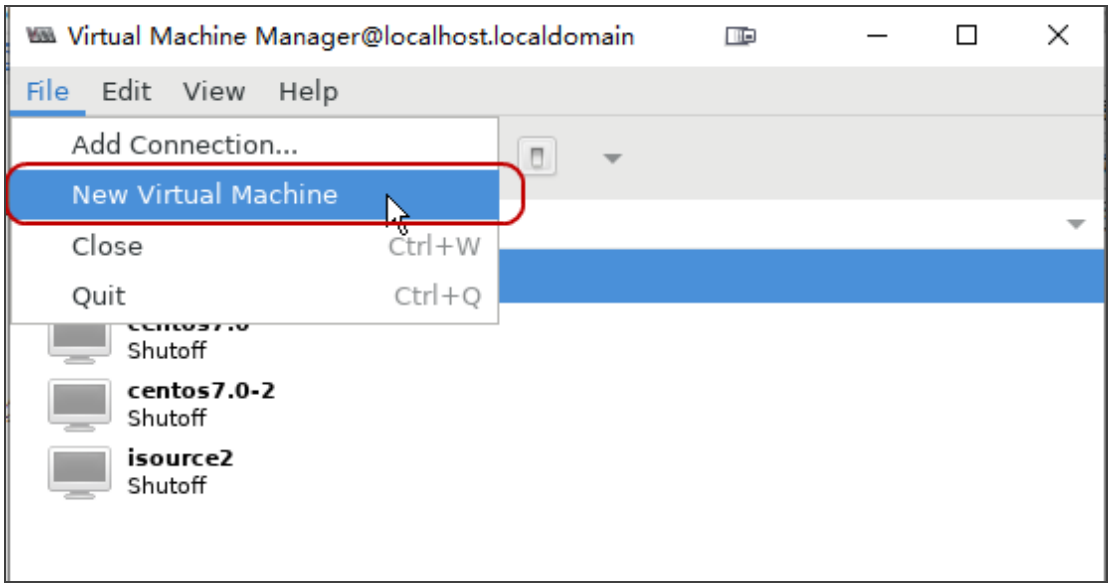
1. 打开MobaXterm主页面，在菜单栏点击“X server”，然后选择“Start X server”，启用X server。
2. 输入命令：**`virt-manager`**。

3. 等待片刻，图形化界面将会打开虚拟机管理图形化界面。

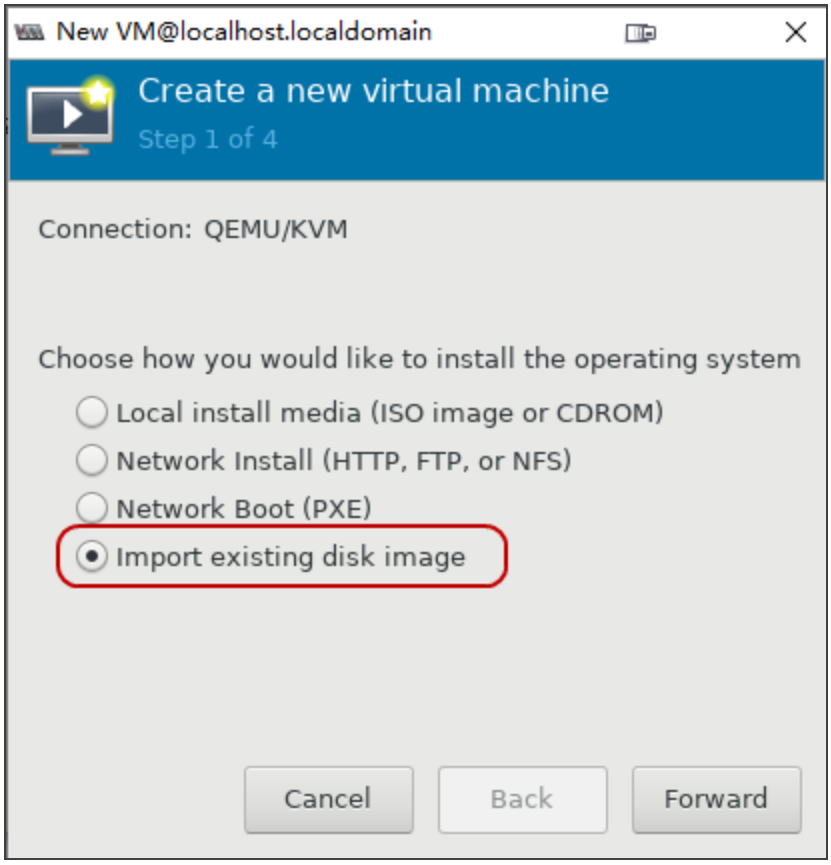


第二步：创建并配置虚拟机

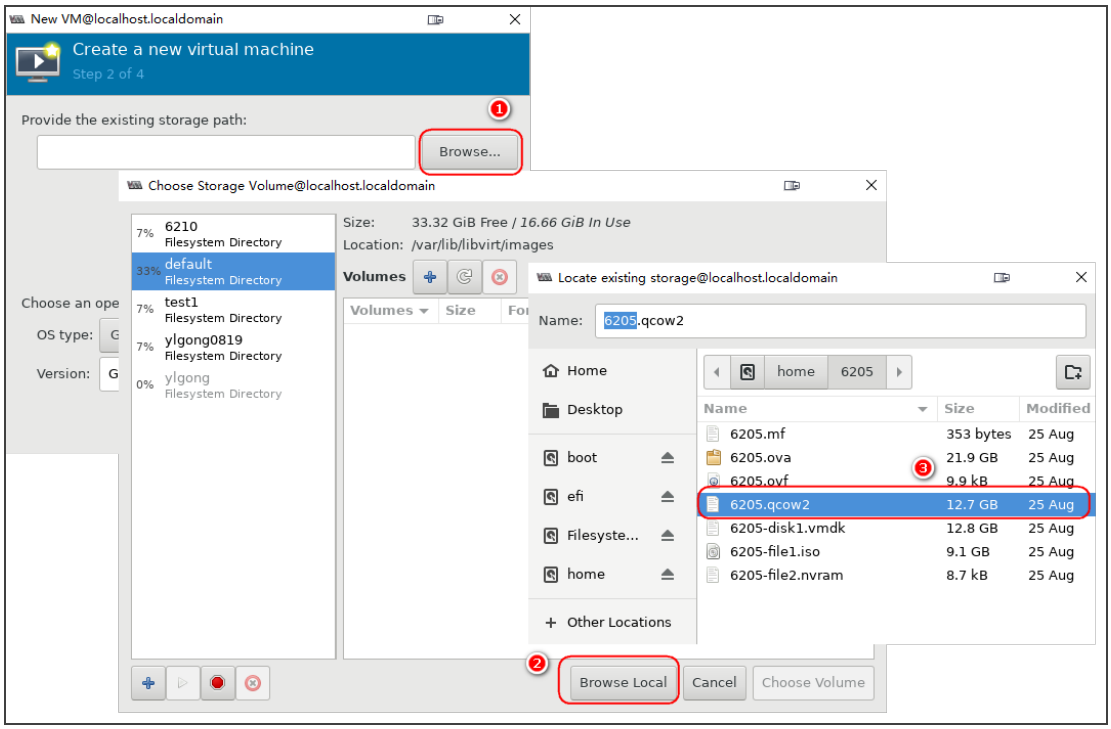
1. 选择“File>New Virtual Machine”，创建虚拟机。



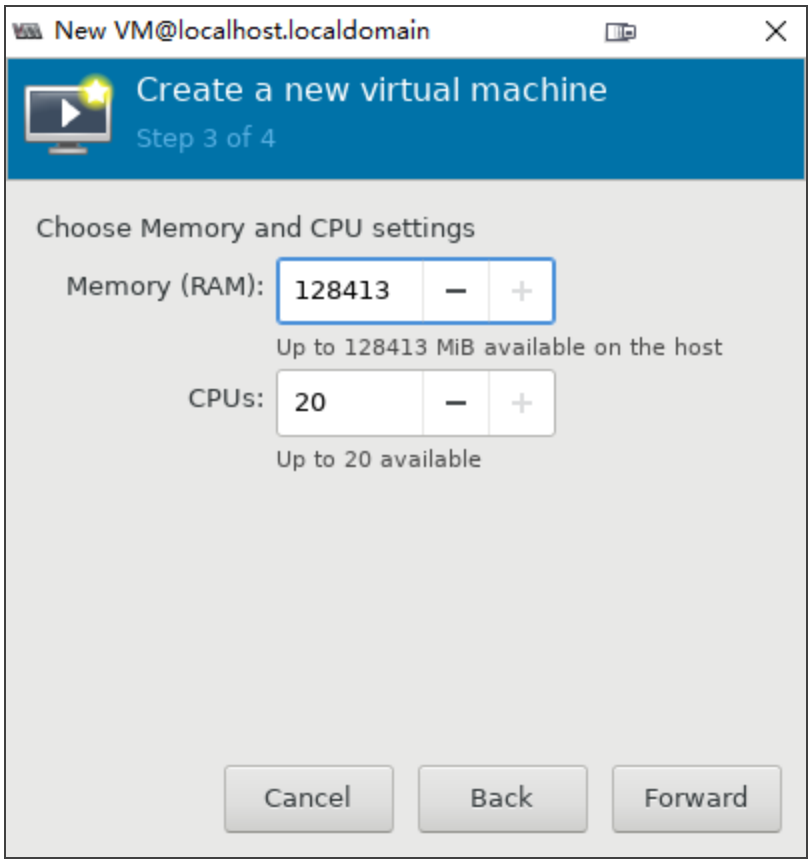
2. 在弹出对话框中，选择“Import existing disk image”，然后点击“Forward”按钮。



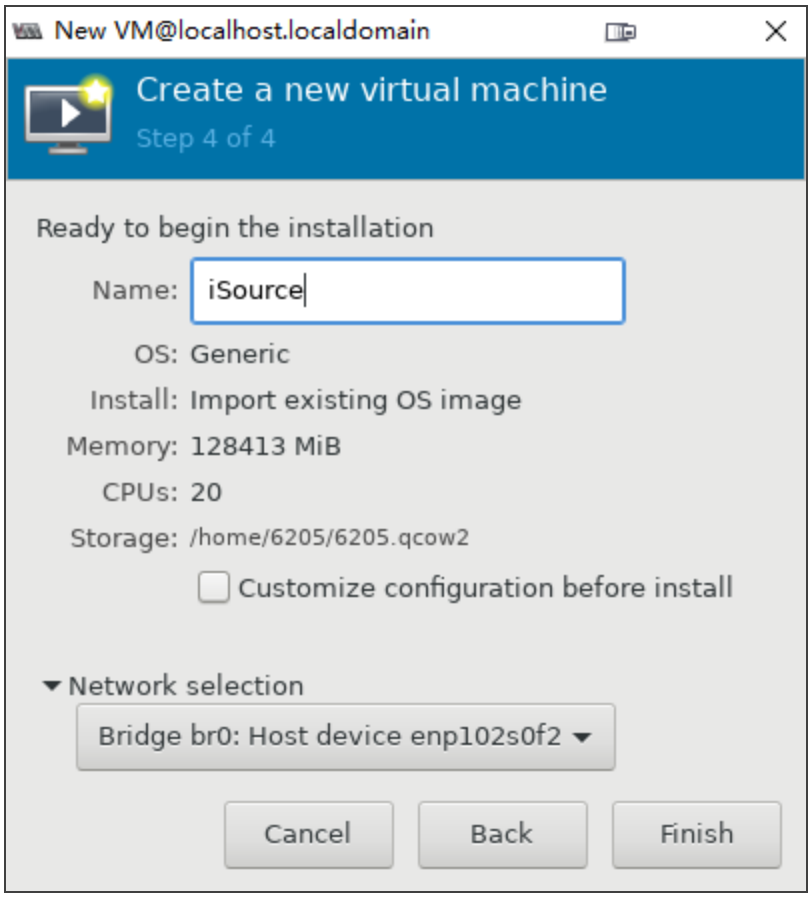
3. 点击“Browse”按钮，然后点击“Browse Local”浏览本地文件，选中已获取的QCOW2格式系统文件。点击“Forward”按钮。



4. 配置虚拟机内存和CPU大小。根据具体安装的产品型号设置内存规格，请参阅产品信息，然后点击“Forward”按钮。



5. 配置虚拟机名称和网络。为虚拟机选择合适网络，根据部署时的实际网络环境进行配置。点击点击“Finish”按钮完成虚拟机的创建。



6. 完成上述配置后，虚拟机将会正常启动。

第三步：配置智源访问地址以及部署系统

1. 输入**show network internal segment**命令检查系统内部IP网段是否和用户网络中的IP地址冲突。如果不冲突，保持当前系统内部IP网段；如果冲突，输入**network internal segment --ip** *subnet/mask* 命令配置网段（掩码必须小于24，例如192.168.82.0/23），并在配置的网段中选择第一个IP地址作为该设备的内部IP地址。

   注意：请确保该步骤中配置的网段内的所有IP地址均不会和用户网络中的IP地址冲突，并且该步骤需要在部署智源平台系统之前进行。在系统部署完成后，请尽量不要修改当前系统的内部IP地址。

2. 为宿主机接口（例如eth0）配置软件化智源的IP地址（例如10.180.0.4），输入以下命令：

   ```
   SG-6000#network ipconfig --interface eth0 --ip 10.180.0.4/24
   ```

（如软件化智源为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6** *X:X:X:X::X/ipv6-prefix*）。

3. 配置默认网关，输入以下命令：

   SG-6000#**network routeconfig --dst** 0.0.0.0/0 **--gateway** 10.180.0.1

   （如使用IPv6类型的IP地址，配置默认网关可使用SG-6000#**network routev6config --dst** *::/0* **--gateway** *X:X:X:X::X*）

4. （可选）如果有多网段管理需求，则为另一个接口配置IP地址，方法同步骤2。

   注意：软件化智源只能存在一个默认网关，因此为了使多网段网络均能正常通信，应根据实际网络拓扑和需求配置相应的路由，方法同步骤3。

5. 输入**show network ipconfig**和**show network routeconfig**命令检查当前接口和路由配置。

6. 输入**deploy standalone**命令并选择系统语言部署智源平台系统。

   注意：系统语言选定后如需修改，请reset设备并重新部署智源平台系统。

第五步：访问智源系统

1. 部署完成后，打开Web浏览器，在地址栏中输入智源系统的IP地址（https://10.180.0.4）并按回车键。

2. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。



注意: 激活状态下的智源系统才能够正常使用，系统激活具体方式，请参阅激活智源系统。

在Windows 10系统终端主机上部署软件化智源

软件化智源系统通过VHD格式封装，可以安装在任意一台Windows 10系统终端主机上。

系统要求和限制

软件化智源的使用要求和限制：

- Windows系统的版本为Windows 10。
- 至少需要64位CPU、安装和运行时需要24个内核、128G内存，具体安装的产品型号规格，请参阅产品信息。

部署步骤

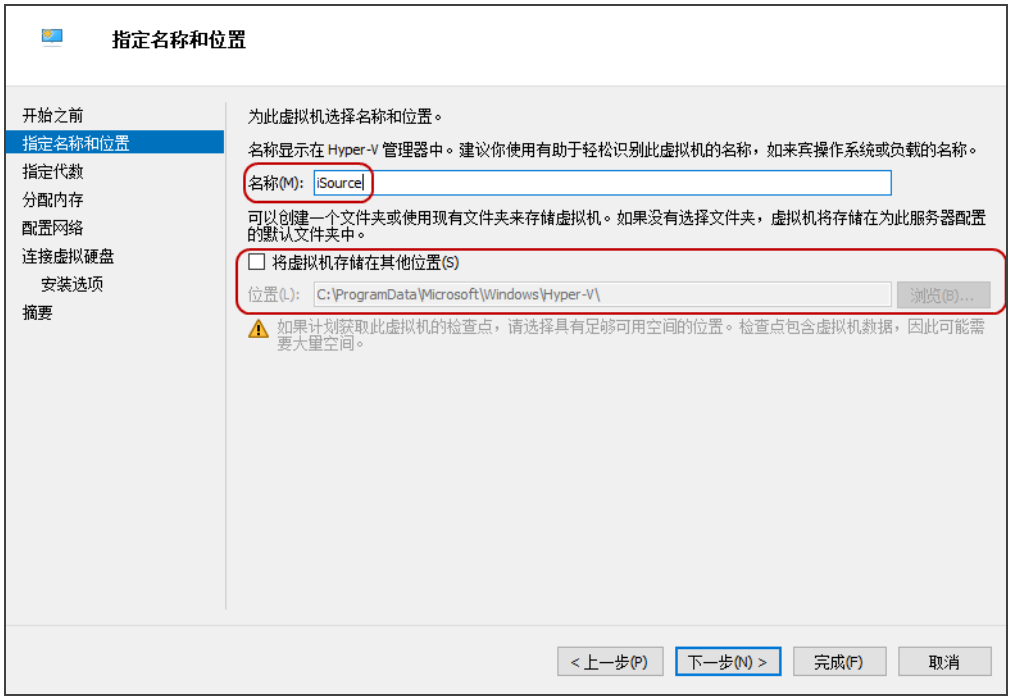
在安装软件化智源之前，请先获取VHD格式系统文件。

第一步：启用Hyper-V功能

1. 在终端主机上，选择“控制面板>程序>程序和功能”，点击“启用或关闭Windows功能”。
2. 在<Windows功能>对话框中，勾选“Hyper-V”复选框，然后点击“确定”按钮，并根据提示完成更新。

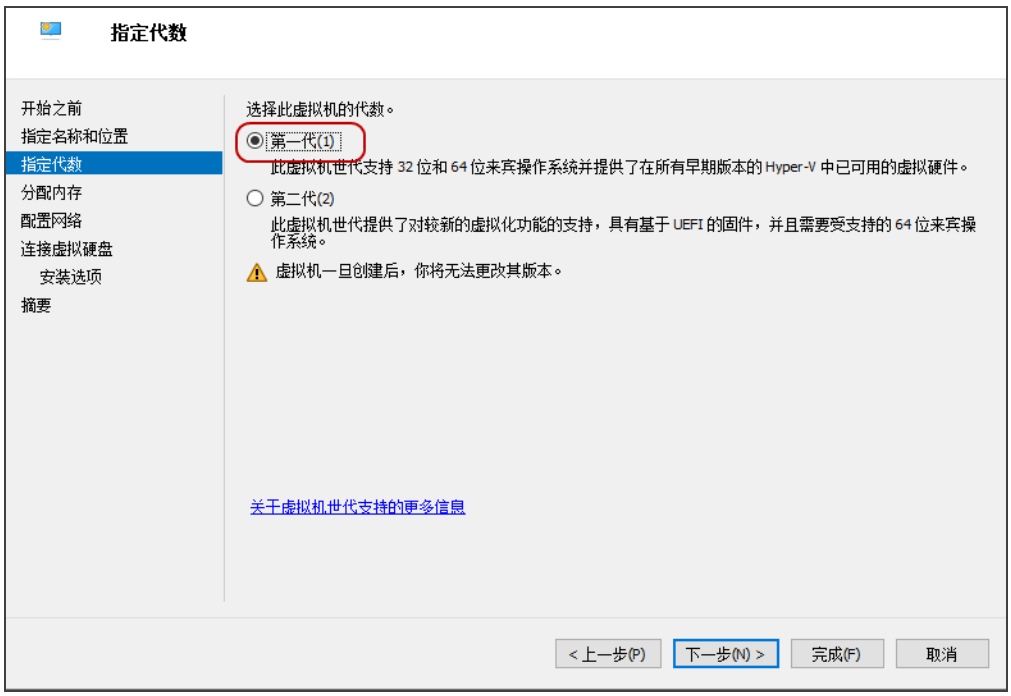
第二步：创建并配置虚拟机

1. 重启终端主机系统后，在任务栏中搜索“Hyper-V管理器”并打开<Hyper-V管理器>页面。
2. 在右侧“操作”框中，点击“新建”按钮，打开<新建虚拟机向导>页面，然后点击“下一步”按钮。
3. 指定名称和位置。在“名称”文本框中指定虚拟机名称；使用默认存储位置或者勾选“将虚拟机存储在其他位置”复选框后点击“浏览”指定自定义存储位置，然后点击“下一步”按钮。

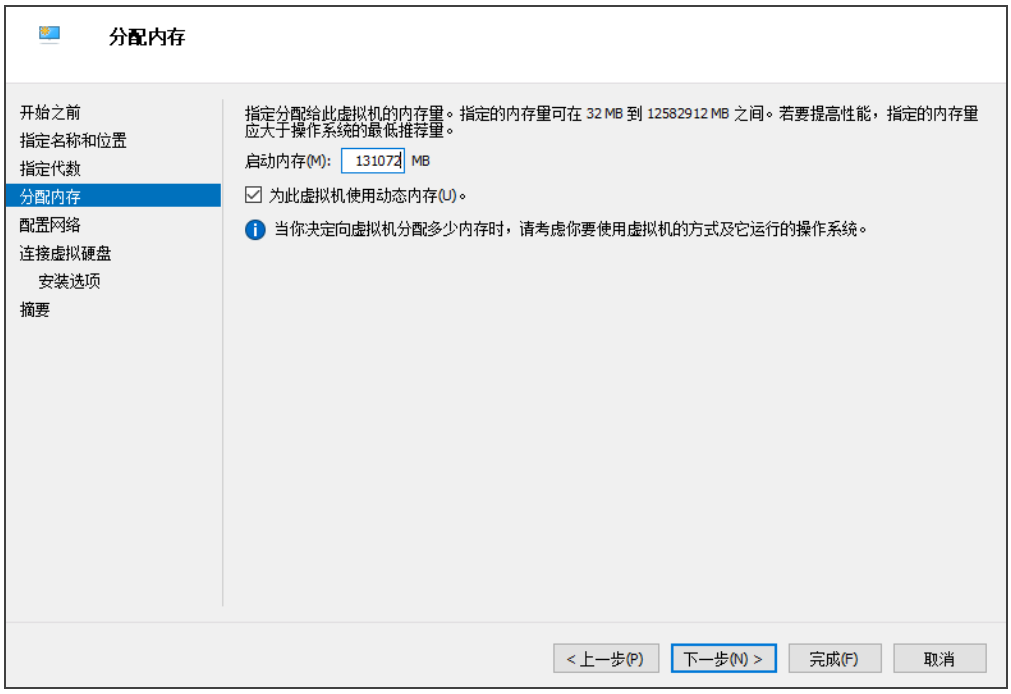


注意：请确保指定的存储位置中有足够的存储剩余空间（20G以上）。

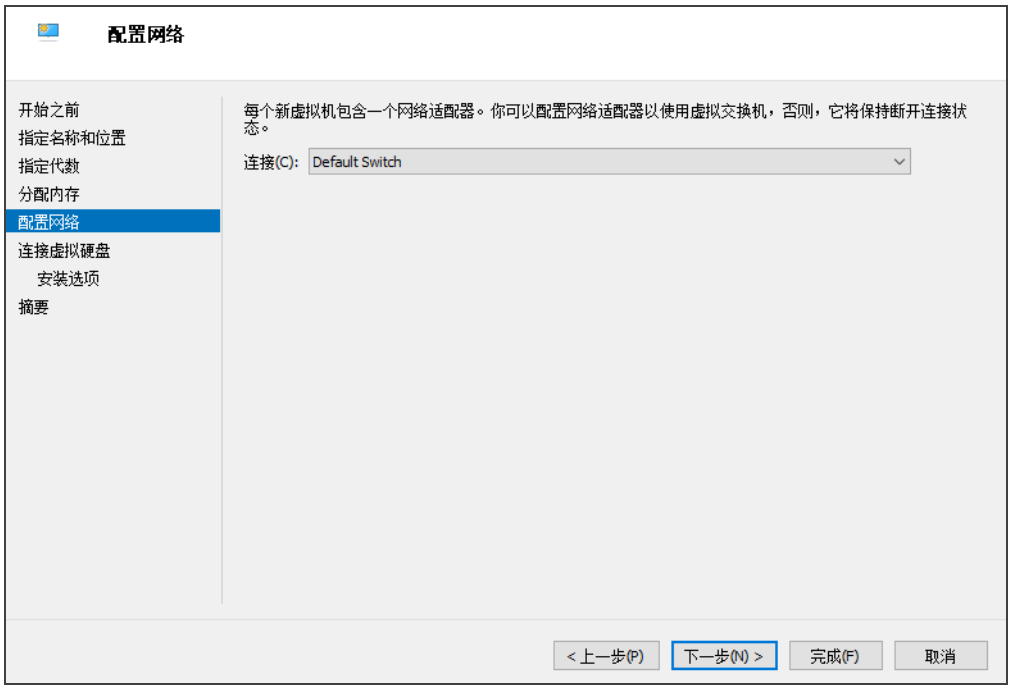
4. 指定代数。默认选择“第一代”，然后点击“下一步”按钮。



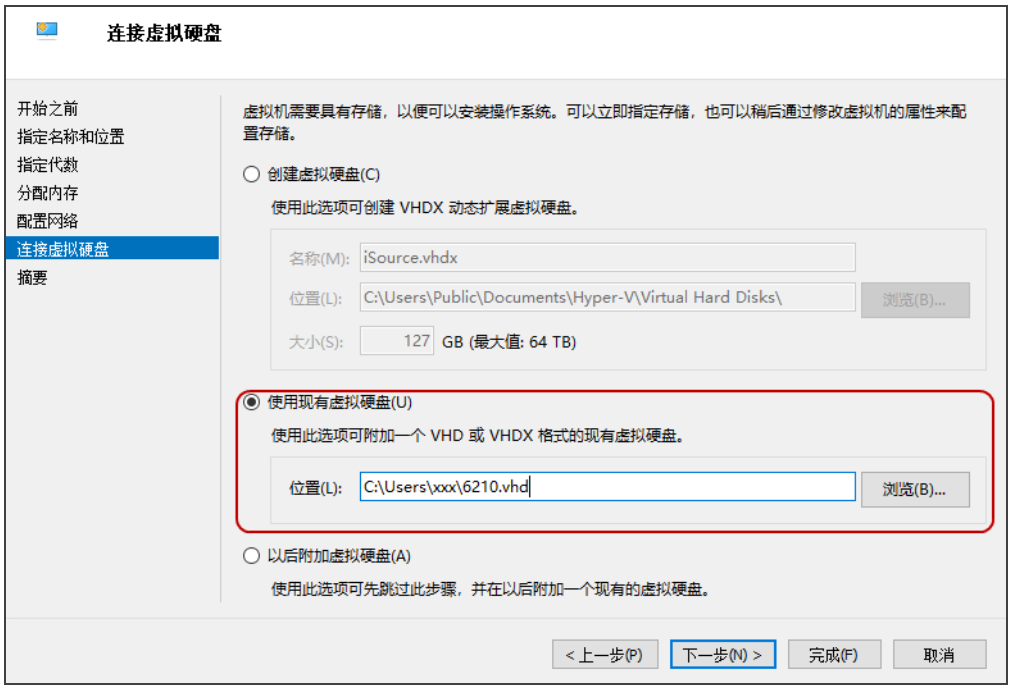
5. 为虚拟机分配内存。在“启动内存”文本框中指定内存大小，根据具体安装的产品型号设置内存规格，请参阅产品信息，然后点击“下一步”按钮。



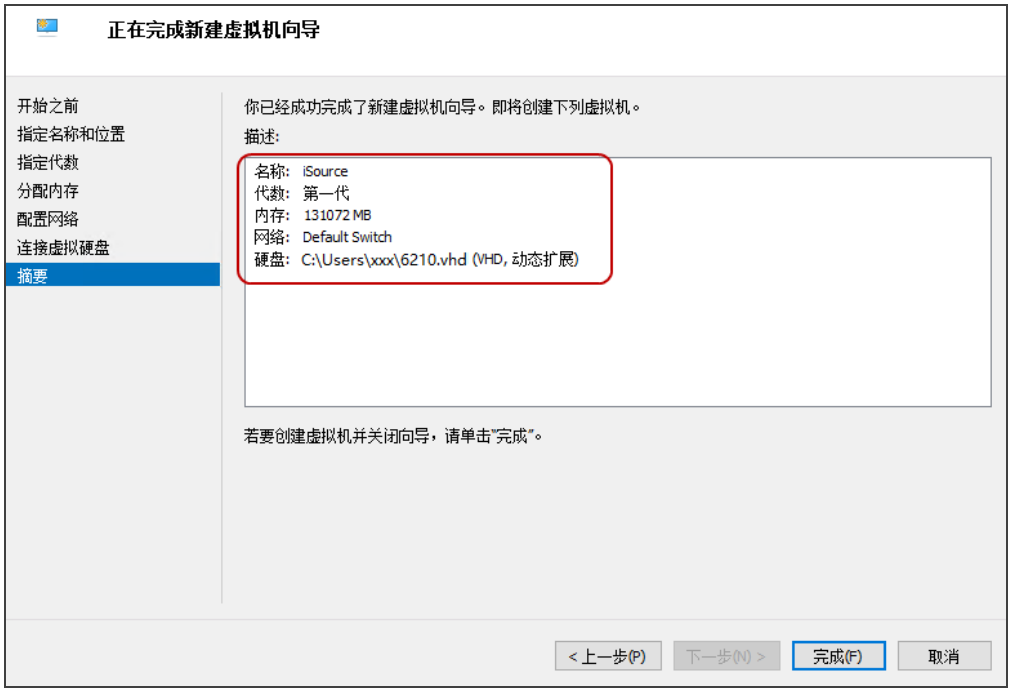
6. 配置网络。为虚拟机选择合适网络，根据部署时的实际网络环境进行配置。点击“下一步”按钮。



7. 连接虚拟硬盘。选择“使用现有虚拟硬盘”，然后点击“浏览”按钮，根据需求选择智源不同型号的VHD格式系统文件。点击“下一步”按钮。



8. 查看摘要。浏览已完成的配置信息，点击“完成”按钮完成虚拟机的创建。

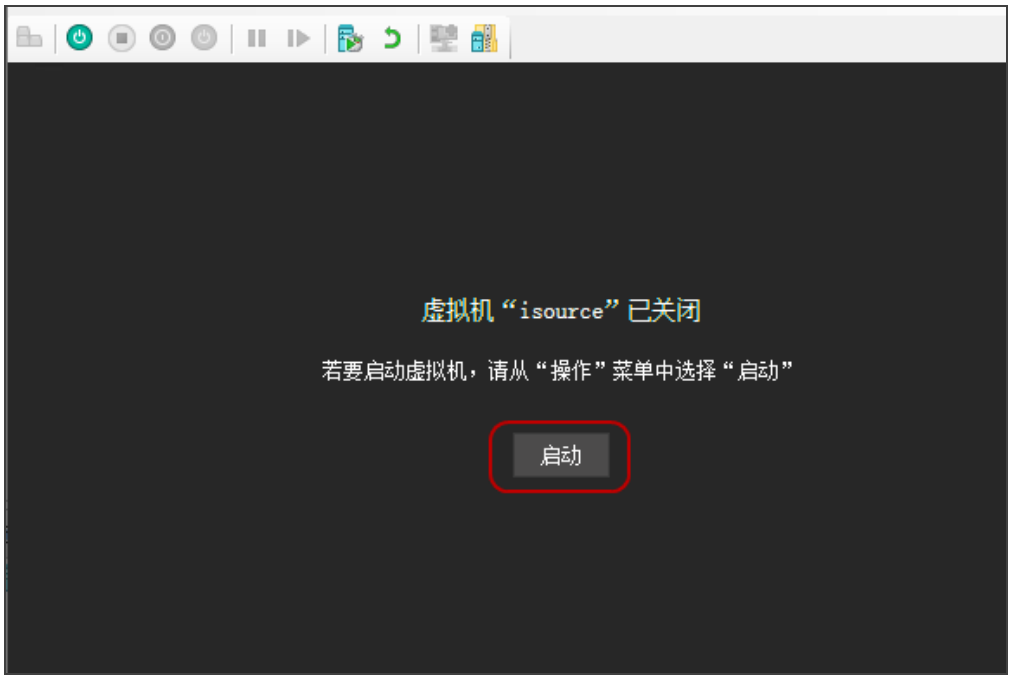


第三步：连接并启动虚拟机

1. 连接前，先确认CPU虚拟处理器数量符合配置要求。
   在<Hyper-V管理器>页面“虚拟机”列表中选择已创建的虚拟机条目，在右侧“操作”框中，点击“设置”，在打开页面的“处理器”部分，确认虚拟处理器的数量是否符合配置要求。如不符合，在页面右侧“虚拟处理器的数量”处进行手动修改。配置要求请参阅产品信息。

2. 在<Hyper-V管理器>页面“虚拟机”列表中选择已创建的虚拟机条目，在右侧“操作”框中，点击“连接”。

3. 在打开的<虚拟机连接>对话框中，点击“启动”按钮。



4. 启动后，输入默认登录用户名/密码：hillstone/hillstone，完成登录。

第四步：配置智源访问地址以及部署系统

1. 输入**show network internal segment**命令检查系统内部IP网段是否和用户网络中的IP地址冲突。如果不冲突，保持当前系统内部IP网段；如果冲突，输入**network internal segment --ip***subnet/mask*命令配置网段（掩码必须小于24，例如192.168.82.0/23），并在配置的网段中选择第一个IP地址作为该设备的内部IP地址。
   注意：请确保该步骤中配置的网段内的所有IP地址均不会和用户网络中的IP地址冲突，并且该步

骤需要在部署智源平台系统之前进行。在系统部署完成后，请尽量不要修改当前系统的内部IP地址。

2. 为宿主机接口（例如eth0）配置软件化智源的IP地址（例如10.180.0.4），输入以下命令：
   `SG-6000#network ipconfig --interface eth0 --ip 10.180.0.4/24`
   （如软件化智源为IPv6类型的IP地址，可使用`SG-6000#network ipv6config --interface eth0 --ipv6X:X:X:X::X/ipv6-prefix`）。

3. 配置默认网关，输入以下命令：
   `SG-6000#network routeconfig --dst 0.0.0.0/0 --gateway 10.180.0.1`
   （如使用IPv6类型的IP地址，配置默认网关可使用`SG-6000#network routev6config --dst::/0 --gatewayX:X:X:X::X`）

4. （可选）如果有多网段管理需求，则为另一个接口配置IP地址，方法同步骤2。
   注意：软件化智源只能存在一个默认网关，因此为了使多网段网络均能正常通信，应根据实际网络拓扑和需求配置相应的路由，方法同步骤3。

5. 输入**deploy standalone**命令并选择系统语言部署智源平台系统。
   注意：系统语言选定后如需修改，请reset设备并重新部署智源平台系统。

第五步：访问智源系统

1. 部署完成后，打开Web浏览器，在地址栏中输入智源的IP地址（https://10.180.0.4）并按回车键。

2. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。



注意: 激活状态下的智源系统才能够正常使用，系统激活具体方式，请参阅激活智源系统。

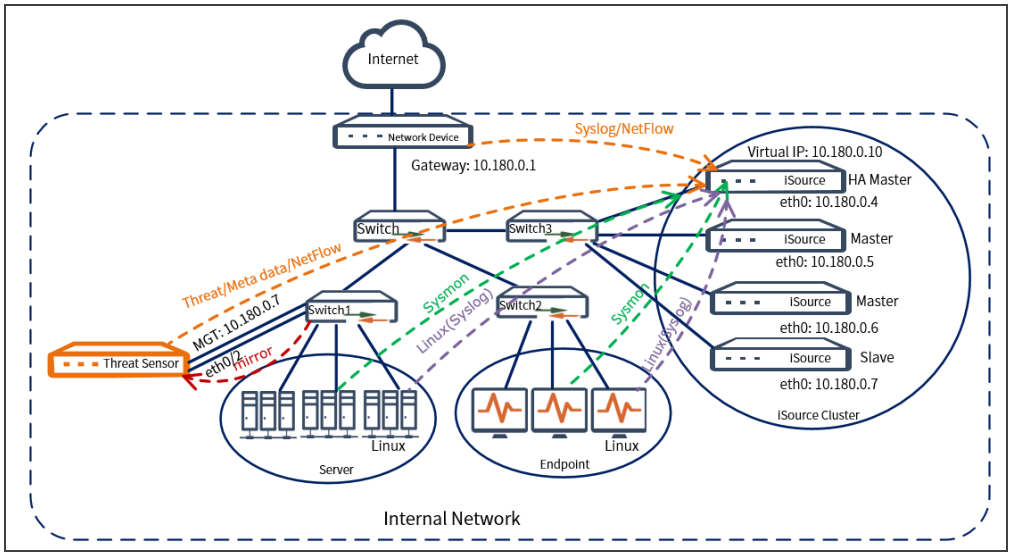
集群部署软件化智源

软件化部署同样支持集群部署，当用户已将软件化智源部署到多台终端主机、虚拟机上，并完成激活后，可将多台设备部署为智源集群。

注意:

- 集群中的所有设备必须部署在同一个二层网络中。
- 确保所有设备均已注册SN且不相同。

本示例中场景见如下组网图：软件化部署4台智源，并且组成智源集群，其中HA Master、Master、Slave等地址以图中标注地址为例。



集群部署软件化智源，请按照如下步骤进行操作：

1. 参考在VMware_ESXi上部署虚拟化智源、在CentOS7系统终端主机上部署软件化智源或者在Windows_10系统终端主机上部署虚拟化智源中步骤，将软件化智源部署到多台终端主机、虚拟机上，选择其中一台设备作为HA Master（例如10.180.0.4）。
2. 部署Master（10.180.0.5），按照以下步骤进行操作：
    1. 通过SSH方式访问设备地址10.180.0.5。
    2. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。
    3. 输入**network ipconfig**命令为宿主机接口（例如eth0）配置智源平台Master的外部IP地址，输入以下命令：

        ```
        SG-6000#network ipconfig --interface eth0 --ip 10.180.0.5/24
        ```

（如软件化智源为IPv6类型的IP地址，可使用SG-6000#**network ipv6config --interface** eth0 **--ipv6***X:X:X:X::X/ipv6-prefix*）。

4. 输入**cluster master**命令指定作为HA Master的智源平台IP地址。

   ```
   SG-6000# cluster master --ip 10.180.0.4
   ```

3. 部署Master（10.180.0.6）、Slave（10.180.0.7），参考上述配置步骤。

4. 将已部署的Master、Slave添加到集群，按照以下步骤进行操作：

   1. 通过SSH方式访问HA Master设备。

   2. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。

   3. 输入**network ha ipconfig**命令配置智源集群的虚拟IP地址（VIP：10.180.0.10），该VIP地址用于对外提供服务，输入以下命令：

      ```
      SG-6000#network ha ipconfig --ip 10.180.0.10
      Config network ha ip success
      ```

      （如智源平台为IPv6类型的IP地址，可使用SG-6000#network ha ipv6 config --ipv6 X:X:X:X::X）

      注意：请确保该VIP地址与交换机在同一个网段。

   4. 输入**cluster add node**命令分别指定各智源Master、Slave的地址，将所有智源Master、Slave加入集群中 。

      添加Master：

      ```
      SG-6000#cluster add node --ip 10.180.0.5
      ```

      添加Master：

      ```
      SG-6000#cluster add node --ip 10.180.0.6
      ```

      添加Slave：

      ```
      SG-6000#cluster add node --ip 10.180.0.7
      ```

   5. 提示成功后，完成智源集群的部署。智源集群即可通过VIP地址对外提供服务。

   6. 输入**show network ha ipconfig**命令查看智源集群的VIP信息。

7. 输入**show cluster**命令查看智源平台集群概要信息，包括集群运行状态、各个智源平台详细信息等 。
8. 打开Web浏览器，在地址栏中输入https://10.180.0.10（即VIP地址）并按回车键。
9. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页 。



注意: 激活状态下的智源系统才能够正常使用，在集群部署中，激活系统需注意以下几点：

- 对于HA Master设备，可使用任意一种方式激活系统；
- 对于Master、Slave设备，仅可通过CLI方式激活系统。

激活智源系统

激活状态下的智源系统才能够正常访问，需完成系统的激活。用户可根据需求，选择激活方式进行激活。

- 在部署系统前，如需激活智源系统，可通过CLI方式激活系统。
- 在部署系统完成后，如需激活智源系统，可通过WebUI方式激活。

通过CLI方式激活

1. 使用SSH方式访问设备。
2. 与设备建立连接后，在弹出的对话框中输入密码“hillstone”，敲回车键，进入CLI配置界面。
3. 输入**bind sn** *SN-string* 命令为该设备绑定SN。

4. 选择激活方式，激活方式包括在线激活和离线激活。

   - 在线激活：如果用户的网络环境已连通网络，推荐使用在线激活方式。

     1. 输入**network dnsconfig** *dns-server-address*命令为该设备配置DNS服务器。

     2. 输入**active online**命令在线激活智源系统。

   - 离线激活：如果用户的网络环境无法使用在线激活方式，可使用离线激活方式。

     1. 输入**active code**命令获取并复制激活码。

     2. 访问http://activation.hillstonenet.com/isource_activesn_offline.html链接进行确认激活，并获取激活结果。



     3. 输入**active offline***激活结果*命令激活智源系统。

通过WebUI方式激活

1. 部署完成后，打开Web浏览器，在地址栏中输入智源的IP地址并按回车键。
2. 输入默认用户名和密码：hillstone和hillstone，并输入图片中的验证码，然后点击“登录”进入设备的主页。
3. 登录后系统自动跳转至激活页面，对智源系统进行激活。
4. 根据需求选择激活方案：正式版激活、试用版激活（本示例以试用版激活为例）。



5. SN注册。在“SN注册码”文本框中输入已申请的SN注册码，请提前向山石网科相关人员进行申请。然后点击“下一步”按钮。



6. 选择激活方式。激活方式包括在线激活和离线激活，如果用户的网络环境已连通网络，推荐用户优先使用“在线激活”方式。



- 在线激活：选择“在线激活”后，点击“激活”按钮。
- 离线激活：如果用户的网络环境无法使用在线激活方式，可选择“离线激活”方式。



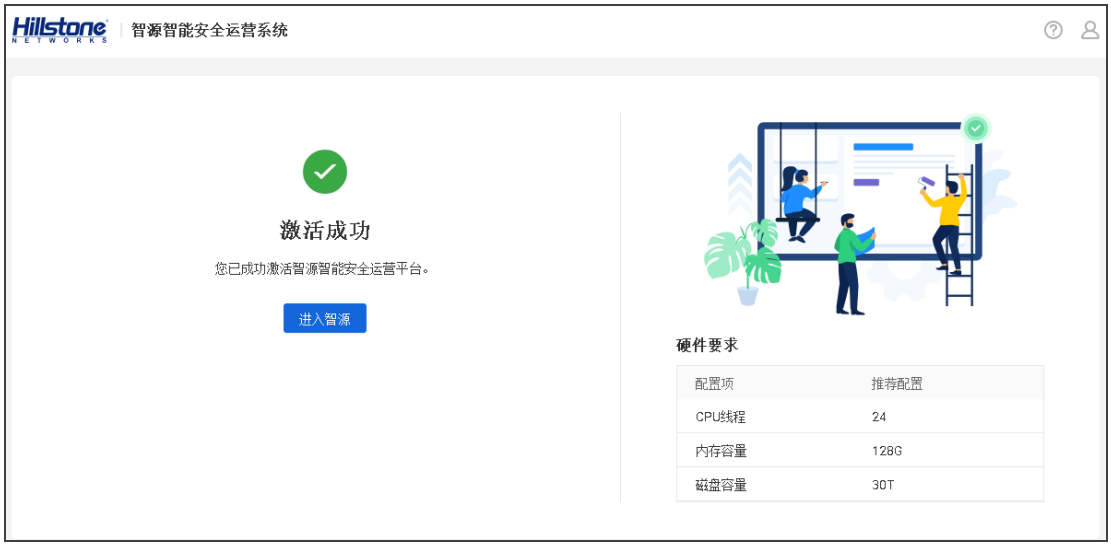
1. 选择“离线激活”，复制表格中的请求码，并点击访问系统提示的链接进行确认激活以获取“SN激活响应串”。



2. 将获取的“SN激活响应串”输入下方“激活密钥”文本框中。

3. 点击“激活”按钮。

7. 提示激活成功后即可点击“进入智源”按钮访问智源系统。



注意: 如果用户使用试用版激活方案激活系统，在过期后，用户再次登录系统时仅可以访问软件激活页面；未过期时，用户可以在系统“系统设置>系统信息”页面中更新激活信息。用户均可以重新修改为“正式版激活”或者在试用版本基础上续期。

- 若选择“正式版激活”，则须使用正式激活的SN注册码激活设备，激活方法同上。
- 若选择“试用版续期”，则需使用正确的试用续期码，延长软件的试用期限。

第2章 态势监控

态势监控通过多种方式、多维度的展示终端和服务器的安全风险状态概览以及相关的威胁事件统计概览。态势监控页面包含以下部分：

- 关注态势
- 资产态势
- 溯源模式
- 流量监控
- 平台总览
- 态势大屏
- 自定义模块

关注态势

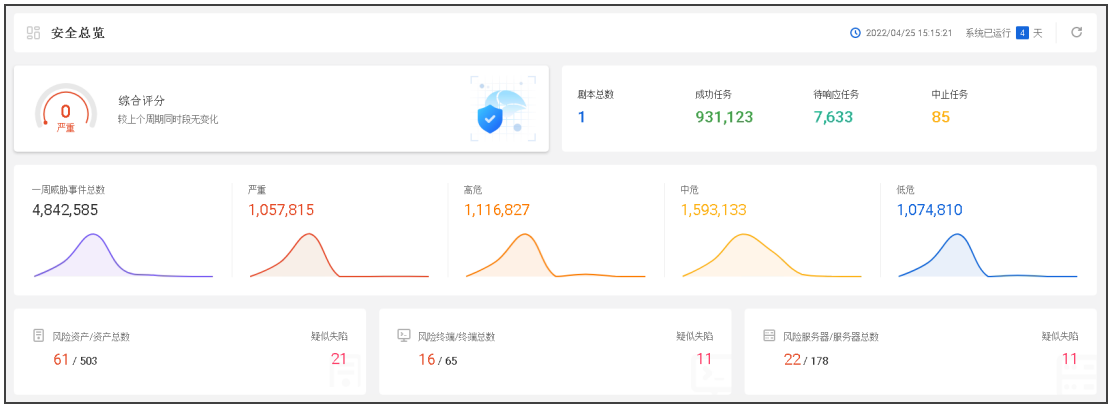
<关注态势>标签页包含告警、安全总览、我的关注、资产态势、威胁事件监控、弱点监控、系统状态监控。

告警



- 展示自动告警、威胁告警、系统告警以及许可证过期告警的未读告警信息个数。
- 点击“查看”按钮，跳转至"告警通知" 在第471页页面，查看告警信息详情。

安全总览



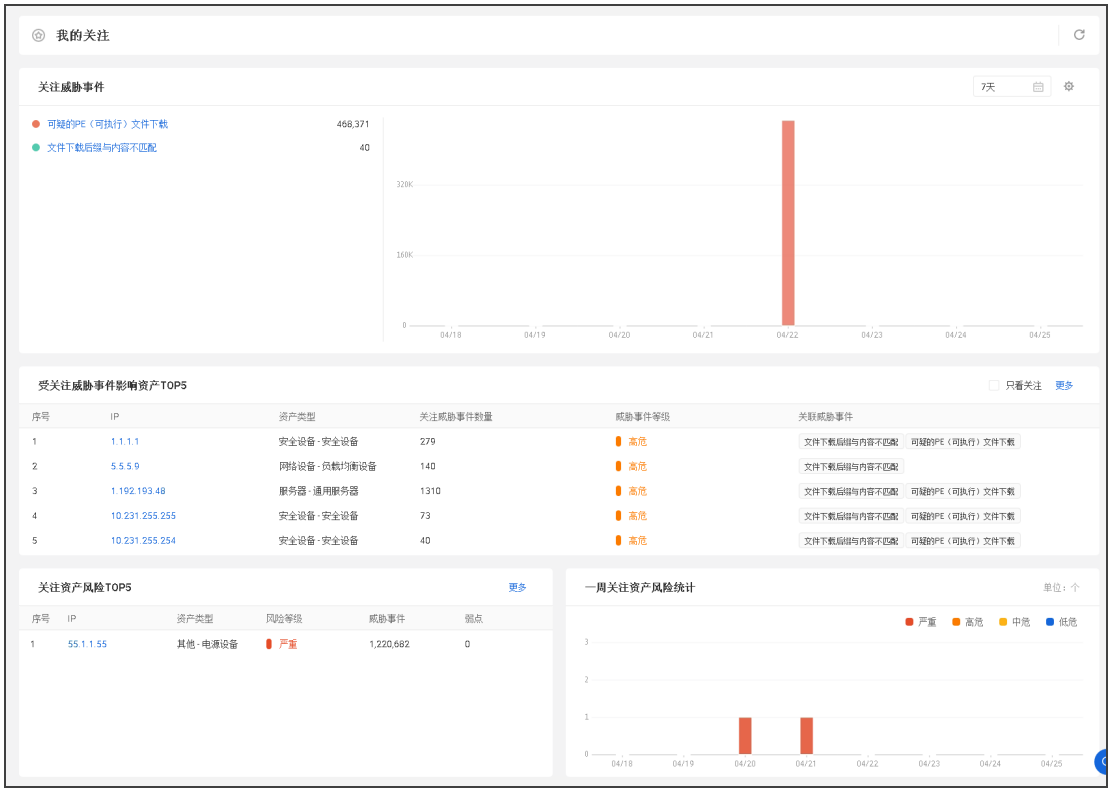
- 该区域右上角显示当前系统时间、系统运行时长。
- 点击 按钮，立即刷新“安全总览”部分的数据。
- 综合评分： 显示系统根据各级别的风险和无风险的终端/服务器比例所计算出的分数。
- 剧本总览：
  - 剧本总数： 显示创建的剧本总数。
  - 成功任务： 显示成功响应的任务数量。
  - 待响应任务：显示待响应任务数量。
  - 中止任务：显示中止任务的数量。
  - 点击数字跳转至"剧本管理" 在第216页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"剧本管理" 在第216页页面，查看所有剧本/成功任务/待响应任务/中止任务信息。
- 威胁事件总览：
  - 显示最近一周内已解决和未解决的威胁事件总数、按照严重程度显示各级别威胁事件的数量以及趋势图。
  - 点击数字跳转至"威胁" 在第115页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"威胁" 在第115页页面，查看最近一周内对应各级别威胁事件信息。
  - 鼠标悬停在趋势图上，显示对应时间点的威胁事件数量。

- 资产总览：
    - 风险资产：显示存在未解决威胁事件或者弱点的资产数量。点击数字跳转至"全部资产风险" 在第185页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"全部资产风险" 在第185页页面，查看风险资产列表详细信息。
    - 资产总数：显示所有手动录入和主动探测的资产总数量。 点击数字跳转至"资产列表" 在第339页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"资产列表" 在第339页页面，查看资产列表详细信息。
    - 疑似失陷：显示经过失陷评估判定的疑似失陷资产数量。点击数字跳转至"全部资产风险" 在第185页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"全部资产风险" 在第185页页面，查看疑似失陷的资产列表详细信息。
- 终端总览：
    - 风险终端：显示存在未解决威胁事件或者弱点的终端数量。点击数字跳转至"终端风险" 在第203页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"终端风险" 在第203页页面，查看风险终端列表详细信息。
    - 终端总数：显示所有系统自动识别和自定义的终端总数量。 点击数字跳转至"资产列表" 在第339页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"资产列表" 在第339页页面，查看终端列表详细信息。
    - 疑似失陷：显示经过失陷评估判定的疑似失陷终端数量。点击数字跳转至"终端风险" 在第203页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"终端风险" 在第203页页面，查看疑似失陷的终端列表详细信息。
- 服务器总览：
    - 风险服务器：显示存在未解决威胁事件或者弱点的服务器数量。点击数字跳转至"服务器风险" 在第194页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"服务器风险" 在第194页 页面，查看风险服务器列表详细信息。
    - 服务器总数： 显示所有系统自动识别和自定义的服务器总数量。点击数字跳转至"资产列表" 在第339页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"资产列表" 在第339页 页面，查看服务器列表详细信息。

- 疑似失陷：显示经过失陷评估判定的疑似失陷服务器数量。点击数字跳转至"服务器风险" 在第194页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"服务器风险" 在第194页 页面，查看疑似失陷的服务器列表详细信息。

我的关注

显示用户关注的威胁事件、受关注威胁事件影响的资产TOP5以及关注风险资产TOP5。



- 点击 按钮，立即刷新“我的关注”部分的数据。
- 关注威胁事件
  - 默认5分钟自动刷新关注列表。
  - 点击 按钮，打开<编辑关注>页面，选择需要重点关注的威胁事件。点击 按钮，显示为 时，即表示已添加为关注。系统最多支持关注10条威胁事件。
  - 点击时间控件下拉框选择威胁事件发生的时间范围，可以选择24小时、7天或30天。系统默认时间范围为7天。

    - 左侧显示威胁事件的名称和总数，点击数字跳转至"事件列表" 在第136页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"事件列表" 在第136页页面，查看系统检测出的所有对应该名称的威胁事件列表。
    - 右侧柱状图显示指定时间内威胁事件的数量，鼠标悬停在柱状图上可以查看对应时间点上具体威胁事件的数量。
- 受关注威胁事件影响TOP5：统计30天内的数据，并展示排名前5的资产。首先根据威胁事件等级进行排序；等级相同时，再根据严重等级的关注威胁事件数量排序；若严重等级的关注威胁事件数量也相同，再根据高危等级的关注威胁事件数量排序；同样按此方法，再依次根据中危、低危的关注威胁事件数量排序，综合获得排名前5的资产。
    - 勾选“只看关注”复选框，筛选出关注资产中排名前5的资产。取消勾选，从全部资产中筛选出前5的资产。默认情况不勾选。
    - “关联威胁事件”列中展示该资产上数目最多的两件威胁事件的名称。
    - 点击资产的IP，跳转至"全部资产风险" 在第185页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"全部资产风险" 在第185页页面，查看对应资产的详细信息。
    - 点击“更多”，跳转至"全部资产风险" 在第185页页面，查看30天内的全部风险资产。
- 关注资产风险TOP5：统计30天内的数据，并展示排名前5的资产。首先根据风险等级进行排序；等级相同时，再根据关注资产中严重等级的威胁事件和弱点数量排序；若数量也相同，再根据高危等级的威胁事件和弱点数量排序；同样按此方法，再依次根据中危、低危的威胁事件和弱点数量排序，综合获得排名前5的资产。
    - 点击资产的IP，跳转至"全部资产风险" 在第185页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"全部资产风险" 在第185页页面，查看对应资产的详细信息。
    - 点击“更多”，跳转至"全部资产风险" 在第185页页面，查看30天内被设为重点关注资产的详细信息，按风险等级降序排列。
- 一周关注资产风险统计
    - 柱状图显示一周内重点关注资产上发生风险的数量，点击数字跳转至"全部资产风险" 在第185页页面，查看对应时间点、对应级别的重点关注资产的详细信息。

资产态势



- 点击 按钮，立即刷新“资产态势”部分的数据。
  - 全部
    - 展示风险资产以及疑似失陷资产的数量，点击“查看”跳转至"全部资产风险" 在第185页页面，查看30天内所有风险资产的详细信息，按风险等级降序排列。
    - 圆环图展示了各级别风险资产的大致比例，鼠标悬停在圆环图各部分可以查看各级别风险资产的具体数量。
    - 点击圆环图各部分跳转至"全部资产风险" 在第185页页面，或者在圆环图各部分点击“Ctrl+鼠标左键”在新标签页中打开"全部资产风险" 在第185页页面，查看对应级别风险资产的详细信息。
    - 图例显示各级别风险资产的数量，点击图例或对应的数字，图例变灰色，取消所选风险等级在圆环图的统计展示。
    - 风险资产TOP5列表统计30天内的数据，并展示排名前5的资产。首先根据风险等级进行排序；等级相同时，再根据资产中严重等级的威胁事件和弱点数量排序；若数量也相同，再根据高危等级的威胁事件和弱点数量排序；同样按此方法，再依次根据中危、低危的威胁事件和弱点数量排序，综合获得排名前5的资产。点击“更多”，跳转至"全部资产风险" 在第185页页面，查看30天内所有风险资产的详细信息，按风险等级降序排列。
  - 服务器
    - 展示风险服务器以及疑似失陷服务器的数量，点击“查看”跳转至"服务器风险" 在第194页页面，查看30天内所有风险服务器的详细信息，按风险等级降序排列。

- 圆环图展示了各级别风险服务器的大致比例，鼠标悬停在圆环图各部分可以查看各级别风险服务器的具体数量。
- 点击圆环图各部分跳转至"服务器风险" 在第194页页面，或者在圆环图各部分点击“Ctrl+鼠标左键”在新标签页中打开"服务器风险" 在第194页页面，查看对应级别风险服务器的详细信息。
- 图例显示各级别风险服务器的数量，点击图例或对应的数字，图例变灰色，取消所选风险等级在圆环图的统计展示。
- 风险服务器TOP5列表统计30天内的数据，并展示排名前5的服务器。首先根据风险等级进行排序；等级相同时，再根据资产中严重等级的威胁事件和弱点数量排序；若数量也相同，再根据高危等级的威胁事件和弱点数量排序；同样按此方法，再依次根据中危、低危的威胁事件和弱点数量排序，综合获得排名前5的资产。点击“更多”，跳转至"服务器风险" 在第194页页面，查看30天内所有风险服务器的详细信息，按风险等级降序排列。

- 终端
  - 展示风险终端以及疑似失陷终端的数量，点击“查看”跳转至"终端风险" 在第203页页面，查看30天内所有风险终端的详细信息，按风险等级降序排列。
  - 圆环图展示了各级别风险终端的大致比例，鼠标悬停在圆环图各部分可以查看各级别风险终端的具体数量。
  - 点击圆环图各部分跳转至"终端风险" 在第203页页面，或者在圆环图各部分点击“Ctrl+鼠标左键”在新标签页中打开"终端风险" 在第203页页面，查看对应级别风险服务器的详细信息。
  - 图例显示各级别风险终端的数量，点击图例或对应的数字，图例变灰色，取消所选风险等级在圆环图的统计展示。
  - 风险终端TOP5列表统计30天内的数据，并展示排名前5的终端。首先根据风险等级进行排序；等级相同时，再根据资产中严重等级的威胁事件和弱点数量排序；若数量也相同，再根据高危等级的威胁事件和弱点数量排序；同样按此方法，再依次根据中危、低危的威胁事件和弱点数量排序，综合获得排名前5的资产。点击“更多”，跳转至"终端风险" 在第203页页面，查看30天内所有风险终端的详细信息，按风险等级降序排列。

威胁事件监控

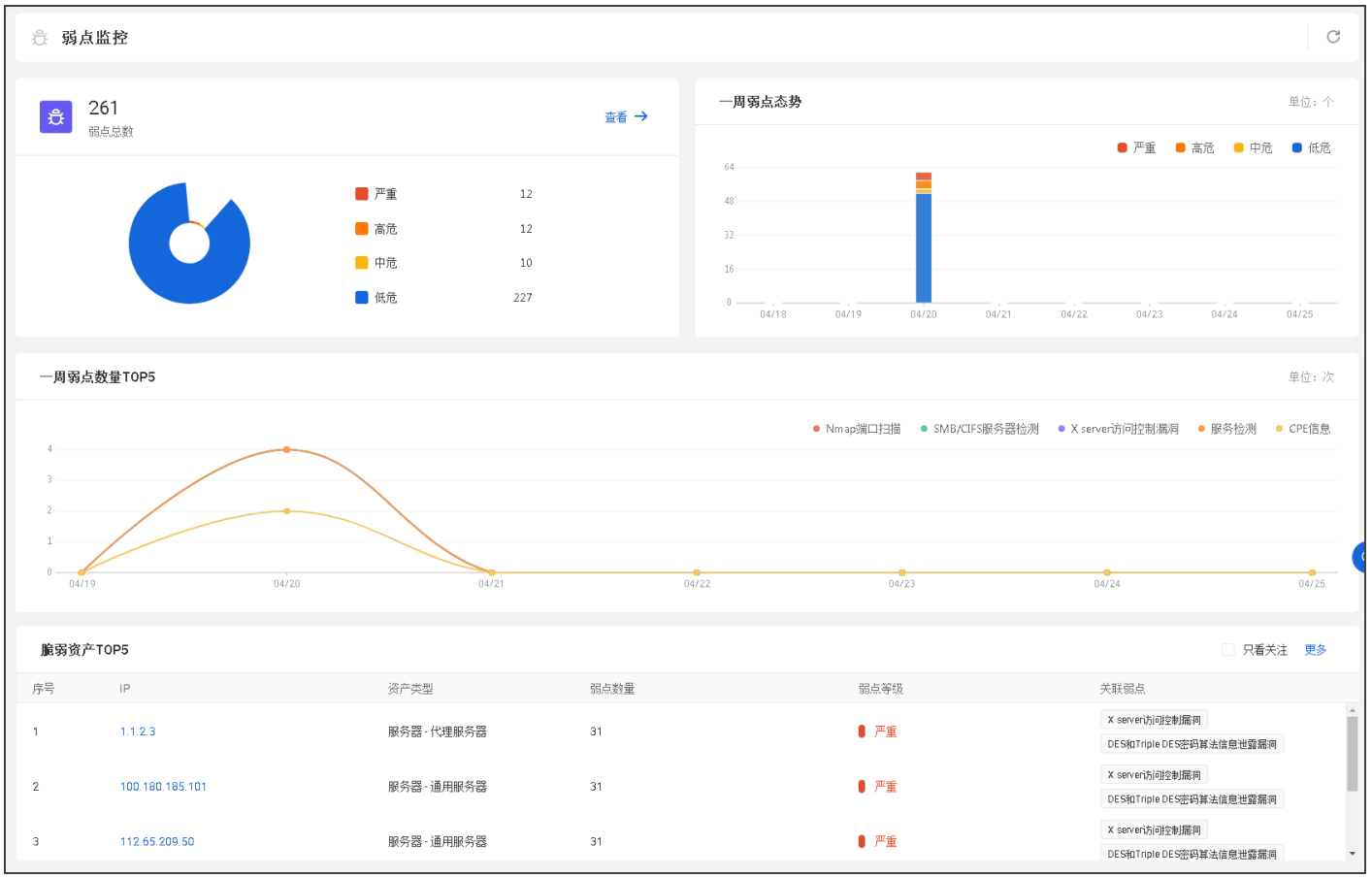


- 威胁事件统计：
  - 展示威胁事件总数。点击“查看”打开"事件列表" 在第136页页面，查看30天内所有威胁事件列表详细信息。
  - 左侧玫瑰图展示所有威胁事件的分布统计结果，右侧展示各方向的威胁事件数量。
  - 点击右侧各级别图例或对应的数字，图例变灰色，取消所选级别在玫瑰图的统计展示。
  - 鼠标悬停在玫瑰图各部分，显示对应方向的威胁事件数量。
  - 点击玫瑰图各部分跳转至"事件列表" 在第136页页面，或者在玫瑰图各部分点击“Ctrl+鼠标左键”在新标签页中打开"事件列表" 在第136页页面，查看对应方向的威胁事件列表详细信息。
- 一周威胁态势：以柱状图形式展示一周内威胁事件的数量统计结果。
  - 鼠标悬停在柱状图上，显示对应时间点的各方向的威胁事件数量。
  - 点击柱状图各部分跳转至"事件列表" 在第136页页面，或者在柱状图各部分点击“Ctrl+鼠标左键”在新标签页中打开"事件列表" 在第136页页面，查看对应时间点、对应方向的威胁事件列表详细信息。
- 一周威胁事件数量TOP5：以曲线图形式展示一周内数量排名前5的威胁事件数量趋势。
  - 鼠标悬停在趋势图上，显示所选时间点的威胁事件TOP5的数量。

- 在趋势图点击对应的时间点跳转至"事件列表" 在第136页页面，或者在趋势图中对应的时间点处点击Ctrl+鼠标左键”在新标签页中打开"事件列表" 在第136页页面，查看所选时间点的聚合威胁事件列表详细信息。

- 点击 按钮，立即刷新“威胁事件监控”部分的数据。

弱点监控



- 弱点统计：

  - 展示弱点总数。点击“查看”打开"弱点分析" 在第162页页面，查看30天内所有主机列表详细信息。

  - 左侧玫瑰图展示所有弱点的分布统计结果，右侧展示各弱点等级的弱点数量。

    - 点击右侧各弱点等级图例或对应的数字，图例变灰色，取消所选弱点等级在玫瑰图的统计展示。
    - 鼠标悬停在玫瑰图各部分，显示对应弱点等级的弱点数量。
    - 点击玫瑰图各部分跳转至"弱点分析" 在第162页页面，或者在玫瑰图各部分点击“Ctrl+鼠标左键”在新标签页中打开"弱点分析" 在第162页页面，查看对应弱点等级的弱点列表详细信息。
- 一周弱点态势：以柱状图形式展示一周内弱点的数量统计结果。
    - 鼠标悬停在柱状图上，显示对应时间点的各弱点等级的弱点数量。
    - 点击柱状图各部分跳转至"弱点分析" 在第162页页面，或者在柱状图各部分点击“Ctrl+鼠标左键”在新标签页中打开"弱点分析" 在第162页页面，查看对应时间点、对应弱点等级的弱点列表详细信息。
- 一周弱点数量TOP5：以曲线图形式展示一周内数量排名前5的弱点数量趋势。
    - 鼠标悬停在趋势图日期对应处，显示一周内数量排名前5的弱点在当天的数量。
    - 在趋势图点击对应的时间点跳转至"弱点分析" 在第162页页面，或者在趋势图中对应的时间点处点击“Ctrl+鼠标左键”在新标签页中打开"弱点分析" 在第162页页面，查看弱点列表详细信息。
- 脆弱资产TOP5：统计30天内的数据，并展示排名前5的资产。首先根据弱点等级进行排序；等级相同时，再根据资产中严重等级的弱点数量排序；若数量也相同，再根据高危等级的弱点数量排序；同样按此方法，再依次根据中危、低危的弱点数量排序，综合获得排名前5的资产。
    - 勾选“只看关注”复选框按钮，筛选出前5的资产中被重点关注的资产。
    - “关联弱点”列展示了该资产上严重程度最高的两个弱点的名称。
    - 点击“更多”，跳转至"弱点分析" 在第162页页面，查看存在弱点的全部资产。
    - 点击资产的IP，跳转至"弱点分析" 在第162页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"弱点分析" 在第162页页面，查看对应资产的详细信息。
- 点击  按钮，立即刷新“弱点监控”部分的数据。

系统状态监控

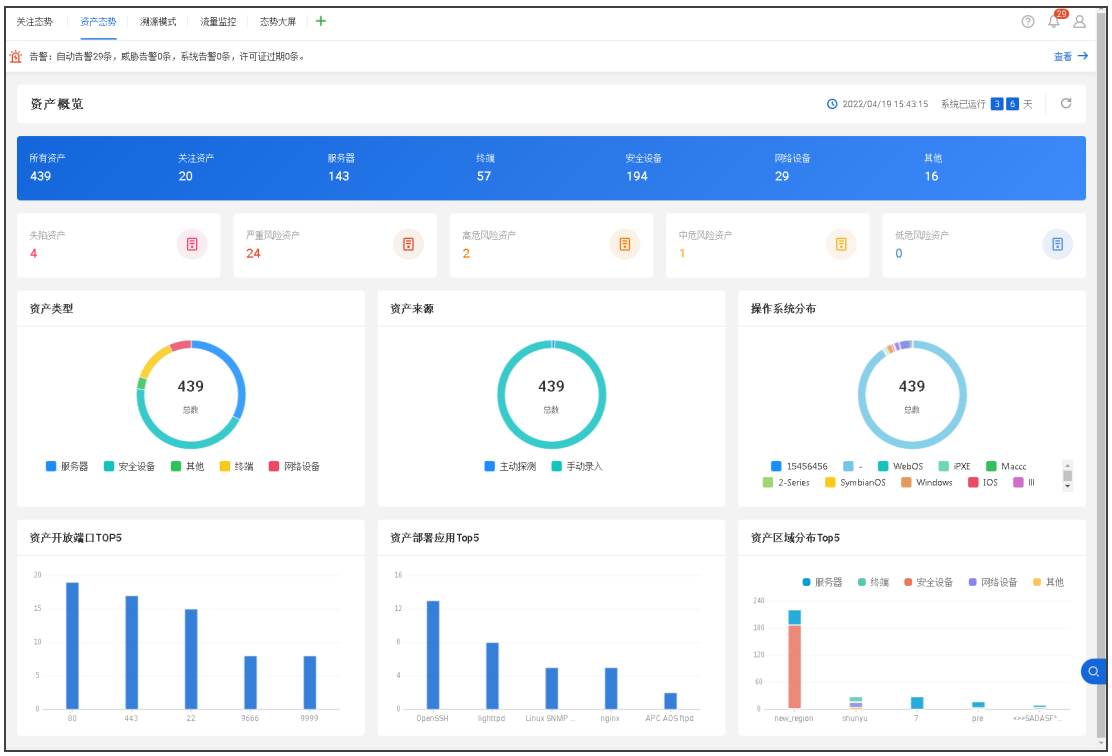


- 系统状态：展示设备CPU利用率、内存利用率以及硬盘使用百分比。点击CPU利用率、内存利用率以及硬盘使用百分比对应的数字，跳转至"集群管理" 在第506页页面，查看当前智源平台的硬件信息或集群中所有设备的硬件信息。
- 点击 按钮，立即刷新“系统状态监控”部分的数据。

资产态势

资产态势页面统计并展示了资产的相关概览。例如，各种类型的资产数量和占比、资产来源的比例、操作系统的分布、开放端口Top5、部署应用Top5以及区域分布Top5。

点击“态势监控 > 资产态势”，进入资产态势页面。



- 该区域右上角显示当前系统时间、系统运行时长。
- 点击 按钮，立即刷新“资产概览”部分的数据。
- 点击页面上方各种类型资产的数字，跳转至“资产管理 > 资产列表”页面，页面上将展示指定类型的资产的信息。例如：点击“关注资产”下的数字，页面跳转至“资产管理 > 资产列表”页面，并展示了全部资产中设为重点关注的资产。
- 点击页面上方各种风险等级的资产对应的数字，跳转至“风险管理 > 全部资产风险”页面，页面上将展示指定风险等级的资产信息。例如：点击“失陷资产”下的数字，页面跳转至“风险管理 > 全部资产风险”页面，并展示全部疑似失陷的资产。
  - 资产类型、资产来源以及操作系统分布圆环图直观展示了不同资产的分布占比情况。
    - 圆环中间显示资产总数。
    - 点击图例，图例变灰，取消所选资产在圆环图中的统计展示。
    - 鼠标悬停在圆环图各部分，显示对应资产的数量或操作系统的数量和占比。
    - 点击圆环图指定部分，跳转至“资产管理 > 资产列表”页面，并展示指定条件的资产的信息。
  - 资产开放端口Top5、资产部署应用Top5以及资产区域分布Top5柱状图直观地展示了资产中排名前5的常见端口、部署应用，以及关联资产数量排名前5的区域。
    - 鼠标悬停在柱状图各部分，显示对应开放端口和部署应用的数量，以及区域中各种类型的资产的具体数量。
    - 点击图例，图例变灰，取消所选资产在柱状图中的统计展示。
    - 点击柱状图指定部分，跳转至“资产管理 > 资产列表”页面，并展示指定条件的资产的信息或指定区域的资产信息。

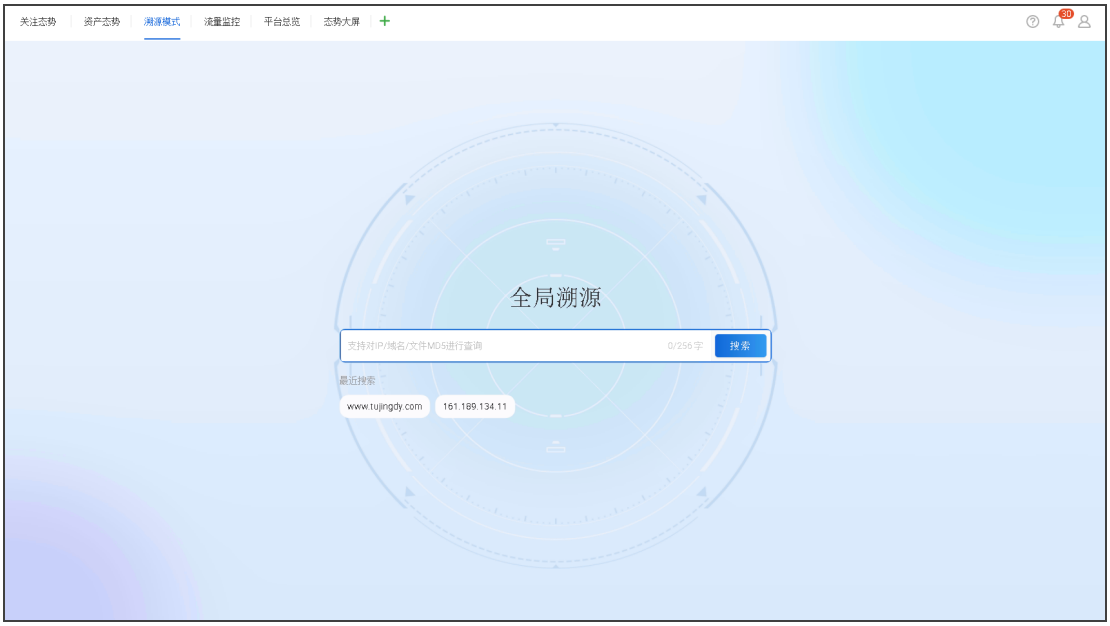
溯源模式

智源平台支持全局溯源功能，可以针对已发生威胁事件的外部IP、内部资产IP、威胁事件的域名以及威胁事件的文件MD5进行查询，查询完成后即可查看和溯源对象相关的所有内容。

全局溯源

全局功能支持两种搜索方式，在<溯源模式>页面搜索或点击页面右下方的按钮进行搜索。

- 点击“态势监控 > 溯源模式”，进入<溯源模式>标签页。



  - 支持对IP、域名、文件MD5进行查询，最多可输入256个字符。输入查询内容后点击“搜索”按钮或按下回车键开始查询。
  - 文本框下展示最近搜索内容，点击指定结果即可开始查询。最多展示6个最近搜索结果。

- 智源平台中所有页面（除<溯源模式>标签页外）均支持全局溯源快捷搜索，点击页面右下方的按钮，打开“全局溯源”对话框。



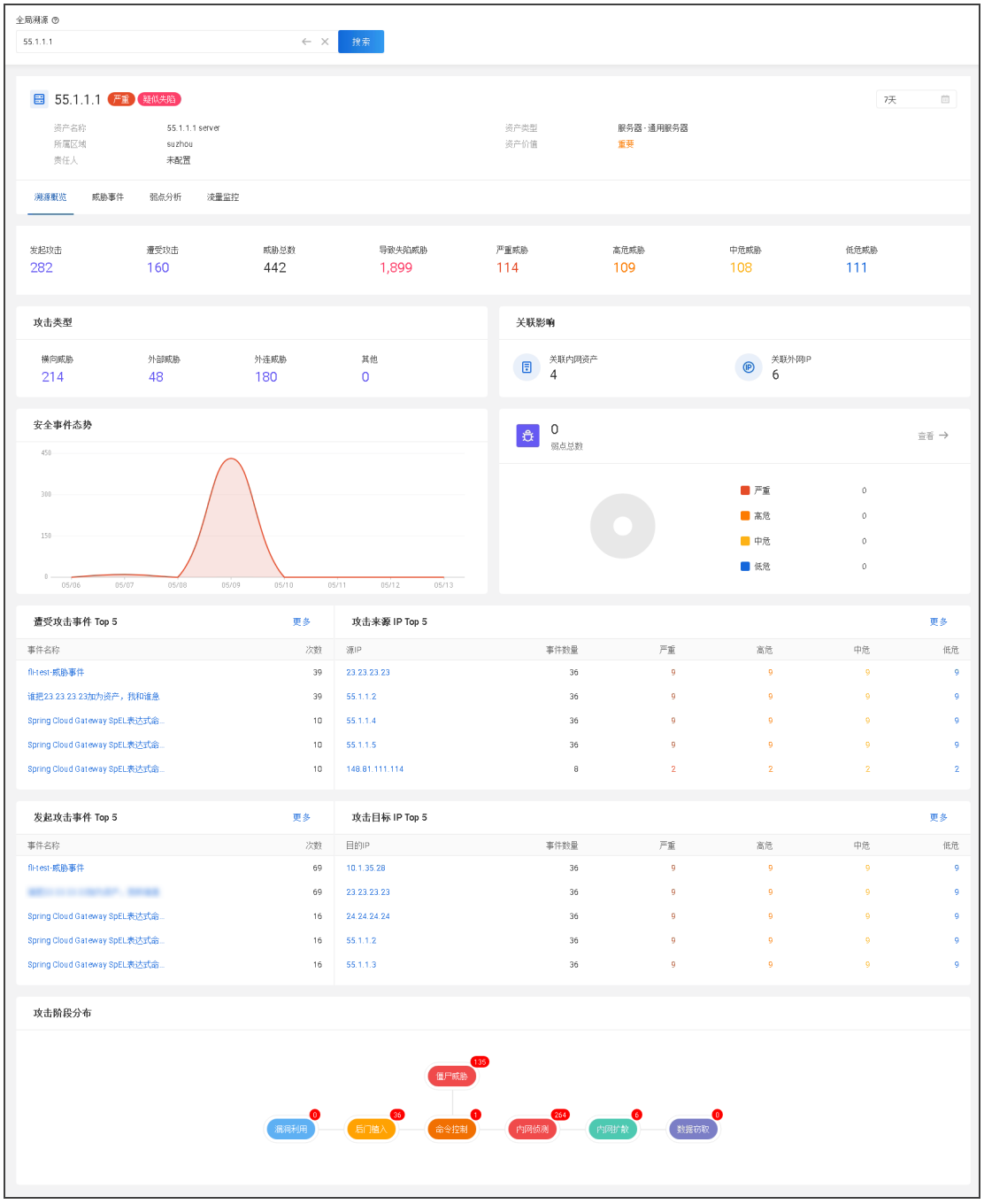
- 支持对IP、域名、文件MD5进行查询，最多可输入256个字符。输入查询内容后点击“搜索”按钮或按下回车键开始查询，并跳转至<溯源模式>页面展示搜索结果。
- 文本框下展示最近搜索内容，点击指定结果即可开始查询。最多展示6个最近搜索结果。

注意: 当设备与其他智源平台进行级联时，即在级联模式下，全局溯源搜索只能搜索出本级平台的数据。

溯源结果

展示指定时间范围内的查询结果，威胁事件数量统计包括已解决和未解决的威胁事件。不同类型的溯源对象展示的页面略有不同，请参照具体页面进行分析。

内部资产


全局溯源
55.1.1.1
搜索
55.1.1.1
严重
疑似失陷
7天
资产名称
55.1.1.1 server
资产类型
服务器-通用服务器
所属区域
suzhou
资产价值
重要
责任人
未配置
溯源概览
威胁事件
弱点分析
流量监控
发起攻击
282
遭受攻击
160
威胁总数
442
导致失陷威胁
1,899
严重威胁
114
高危威胁
109
中危威胁
108
低危威胁
111
攻击类型
横向威胁
214
外部威胁
48
外连威胁
180
其他
0
关联影响
关联内网资产
4
关联外网IP
6
安全事件态势
0
弱点总数
查看
严重
0
高危
0
中危
0
低危
0
遭受攻击事件 Top 5
更多
攻击来源 IP Top 5
更多
事件名称
次数
源IP
事件数量
严重
高危
中危
低危
fl-test-威胁事件
39
23.23.23.23
36
9
9
9
9
谁把23.23.23.23加为资产，我和谁急
39
55.1.1.2
36
9
9
9
9
Spring Cloud Gateway SpEL表达式命...
10
55.1.1.4
36
9
9
9
9
Spring Cloud Gateway SpEL表达式命...
10
55.1.1.5
36
9
9
9
9
Spring Cloud Gateway SpEL表达式命...
10
148.81.111.114
8
2
2
2
2
发起攻击事件 Top 5
更多
攻击目标 IP Top 5
更多
事件名称
次数
目的IP
事件数量
严重
高危
中危
低危
fl-test-威胁事件
69
10.1.35.28
36
9
9
9
9
69
23.23.23.23
36
9
9
9
9
Spring Cloud Gateway SpEL表达式命...
16
24.24.24.24
36
9
9
9
9
Spring Cloud Gateway SpEL表达式命...
16
55.1.1.2
36
9
9
9
9
Spring Cloud Gateway SpEL表达式命...
16
55.1.1.3
36
9
9
9
9
攻击阶段分布
僵尸威胁
139
漏洞利用
0
后门植入
35
命令控制
1
内网侦测
264
内网扩散
6
数据窃取
0

- 页面上方展示资产的IP、风险等级、名称、所属区域、资产类型、资产价值以及责任人等信息。
- 页面右上方选择查看威胁事件信息的时间范围。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- **溯源概览**：
  - 总览：展示指定时间内该资产上发生的威胁事件总数、发起攻击、遭受攻击、各级别威胁事件的数量，以及该资产类型对应评估时间前30天内导致该资产失陷的威胁事件数量。
    - 点击威胁总数对应的数字，将跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击发起攻击对应的数字，系统将根据源IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击各级别威胁对应的数字，系统将根据级别作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击导致失陷威胁对应的数字，将跳转至页面下方<导致失陷威胁事件>标签页的威胁事件列表。
  - 攻击类型：展示指定时间内各种攻击类型的数量。点击对应的数字，系统将根据方向作为筛选条件筛选对应的威胁事件，并跳转至<威胁事件>标签页的威胁事件列表。
  - 关联影响：展示指定时间内该资产关联的内网资产和外网IP数量。
  - 安全事件态势：以曲线图的形式展示指定时间内该资产上发生威胁的趋势，鼠标悬停在曲线图上可以查看指定时间节点的威胁数量。
  - 弱点：玫瑰图展示指定时间内该资产上发现的弱点的分布统计结果，上方展示弱点总数，右侧展示各弱点等级的弱点数量。
    - 点击右侧各弱点等级图例或对应的数字，图例变灰色，取消所选弱点等级在玫瑰图的统计展示。

- 鼠标悬停在玫瑰图各部分，显示对应级别的弱点数量。
- 点击玫瑰图各部分，可跳转至<弱点分析>标签页，查看弱点列表中对应弱点等级的弱点详细信息。
- 点击“查看”按钮，可跳转至<弱点分析>标签页弱点列表。

- 遭受攻击事件 Top5：展示指定时间内对该资产发起攻击次数排名前5的威胁事件。
  - 点击威胁事件的名称，系统将根据威胁事件名称和目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
  - 点击“更多”，系统将根据目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表，查看按名称聚合的威胁事件。
- 攻击来源IP Top5：展示指定时间内对该资产发起攻击次数排名前5的IP以及攻击次数。
  - 点击IP，系统将根据源IP和目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
  - 点击“更多”，系统将根据目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表，查看按名称聚合的威胁事件。
- 发起攻击事件 Top5：展示指定时间内该资产发起的攻击次数排名前5的威胁事件。
  - 点击威胁事件的名称，系统将根据威胁事件名称和源IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
  - 点击“更多”，系统将根据源IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表，查看按名称聚合的威胁事件。
- 攻击目标 IP Top5：展示指定时间内遭受该资产攻击次数排名前5的IP以及攻击次数。
  - 点击IP，系统将根据源IP和目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
  - 点击“更多”，系统将根据源IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表，查看按名称聚合的威胁事件。
- 攻击阶段分布：展示指定时间周期内该资产上发生威胁事件的攻击阶段分布，各攻击阶段右上角数字表示处于该阶段的威胁事件数量。

- **威胁事件**：展示指定时间内该资产上发生的威胁事件详情。
  - 点击上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
  - 点击“聚合”处下拉菜单，选择列表所显示的内容的聚合方式，包括不聚合、按名称、按源IP以及按目的IP。
  - <威胁事件>标签页：以列表的方式展示指定时间内该资产上发生的已解决和未解决威胁事件。具体操作，可参阅事件列表部分。
  - <导致失陷威胁事件>标签页：展示该资产类型评估时间前30天内，导致该资产失陷的威胁事件。点击威胁事件名称，打开威胁事件详情页面，查看所选威胁事件的详细信息。
  - <威胁透视镜>标签页：以图标和箭头连接线的形式展示指定时间内该资产上发生的威胁事件之间的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。点击指定的IP地址，查看该威胁事件的源、目的IP，以及与源、目的IP关联的威胁事件Top5。关联威胁事件Top5按照级别降序排列，级别相同的按照发生次数降序排列。
- **弱点分析**：展示指定时间内该资产上的弱点详情。
  - 总览：展示指定时间内该资产上的弱点总数、各等级的弱点数，以及该资产类型评估时间前30天内被利用弱点种类数量。
    - 点击弱点数量对应的数字，系统将全部的弱点显示在页面下方的弱点列表中。
    - 点击各弱点等级对应的数字，系统将根据弱点等级作为筛选条件筛选对应的弱点，显示在页面下方的弱点列表中。
    - 点击被利用弱点对应的数字，系统将全部被利用的弱点显示在页面下方的威胁弱点关联列表中。
  - 点击上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
    - <弱点列表>标签页：下方列表展示资产存在的所有弱点。

- 点击弱点列表中弱点条目后的按钮，或者在弱点详情页面点击“新建工单”按钮，配置对应的工单对弱点进行响应。
- 点击弱点名称链接，打开所选弱点的详情页面，查看该弱点详细信息、简介、处置建议、参考网站以及受影响的主机列表。

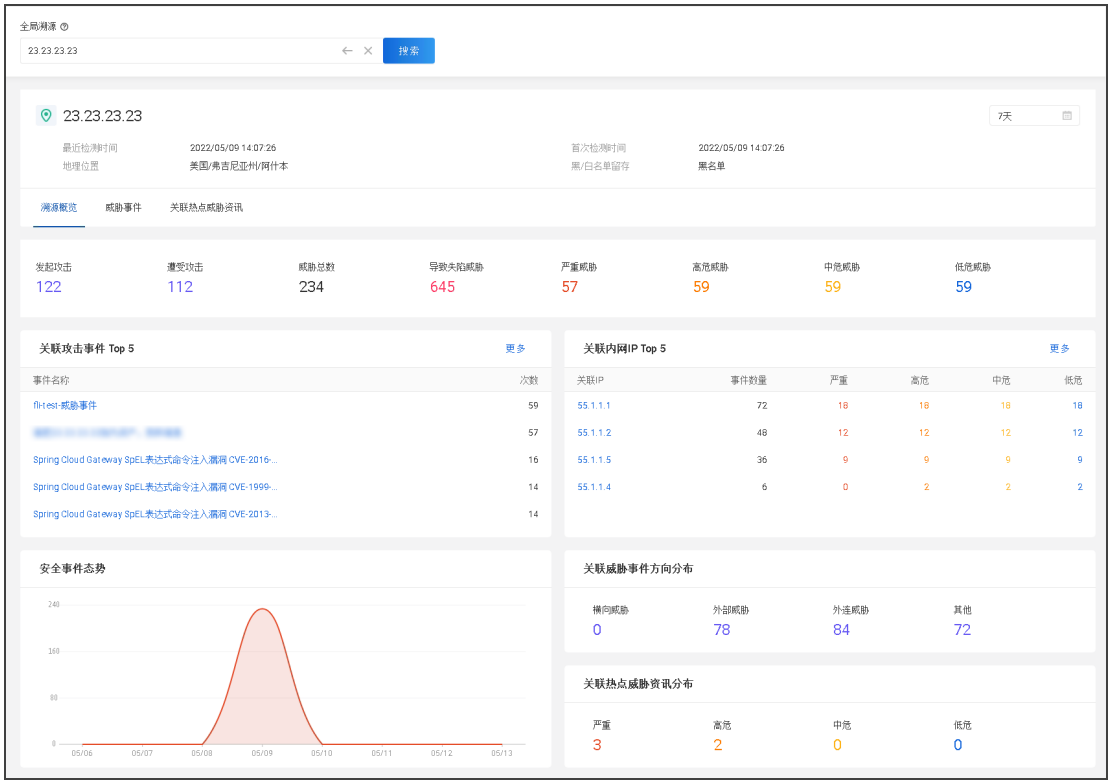
- <威胁弱点关联列表>标签页：展示导致失陷的威胁事件利用的弱点详细列表。

- **流量监控**：展示指定时间内该资产上通过的流量的详细数据。
  - 上方展示流量总数、上行和下行的流量数。
  - 协议流量分布：展示指定时间内流量百分比前5的协议以及其他协议。右侧展示指定协议的百分比和具体流量数值，鼠标悬停在图上可以查看指定协议产生的流量的百分比。
  - <流量趋势>标签页：以曲线图的形式展示指定时间内流量的趋势，鼠标悬停在曲线图上，可以查看指定时间节点上行流量和下行流量的具体数值。
  - <新建连接趋势>标签页：以曲线图的形式展示指定时间内新建连接的趋势，鼠标悬停在曲线图上，可以查看指定时间节点新建连接的具体数值。
  - <关联源IP活动>标签页：以列表的形式展示了指定时间内与该资产有流量交互的源IP信息，包括IP、资产类型、资产名称、区域、流量以及新建连接数。默认按照流量降序排列。
  - <关联目的IP活动>标签页：以列表的形式展示了指定时间内与该资产有流量交互的目的IP信息，包括IP、资产类型、资产名称、区域、流量以及新建连接数。默认按照流量降序排列。

- 点击 按钮，回退到上一次的溯源页面。
- 点击 按钮，清除文本框中的内容。

外部IP/域名/文件MD5

以下图片为外部IP的搜索结果展示页面，不同类型的溯源对象展示的页面略有不同，请参照具体页面进行分析。



- 外部IP类页面上方展示IP地址、威胁标签、恶意标签、最近检测时间、首次检测时间、地理位置、黑/白名单留存情况。
- 域名类页面上方展示域名、域名标签、恶意标签、最近检测时间、首次检测时间以及黑/白名单留存情况。
- 文件MD5类页面上方展示文件MD5值、文件标签、恶意标签、文件大小以及URL信息。
- 页面右上方选择查看威胁事件信息的时间范围。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- “最近检测时间”为指定时间范围内最近一次发生该威胁事件的时间；“首次检测时间”为指定时间范围内最早发生该威胁事件的时间。
- “黑/白名单留存”显示该溯源对象是否在智源平台的黑/白名单中。若在黑名单中，则显示“黑名单”；若在白名单中，则显示“白名单”；若黑名单和白名单中均有该溯源对象，则显示“白名单”；若该溯源对象不在黑名单或白名单中，则显示“未记录”。

- **溯源概览**：
  - 总览：展示指定时间内该溯源对象上发生的威胁事件总数、发起攻击、遭受攻击、导致失陷威胁以及各级别威胁事件的数量。
    - 点击威胁总数对应的数字，将跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击发起攻击对应的数字，系统将根据源IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击各级别威胁对应的数字，系统将根据级别作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击导致失陷威胁对应的数字，将跳转至页面下方<导致失陷威胁事件>标签页的威胁事件列表。
  - 关联攻击事件Top5：展示指定时间内与该溯源对象关联的数量排名前5的威胁事件的名称和发生的次数。
    - 点击事件名称，系统将根据事件名称作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击“更多”，跳转至页面下方<威胁事件>标签页的威胁事件列表，查看按名称聚合的威胁事件。
  - 关联内网IP Top5：展示指定时间内与该溯源对象关联的次数排名前5的内网IP信息，包括IP地址，和该溯源对象相关的威胁事件总量以及各等级的威胁事件的数量。
    - 点击IP，系统将根据IP地址作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
    - 点击“更多”，系统将根据方向为横向威胁、外连威胁、外部威胁作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
  - 安全事件态势：以曲线图的形式展示指定时间内该溯源对象上发生的威胁的趋势，鼠标悬停在曲线图上可以查看指定时间节点的威胁数量。

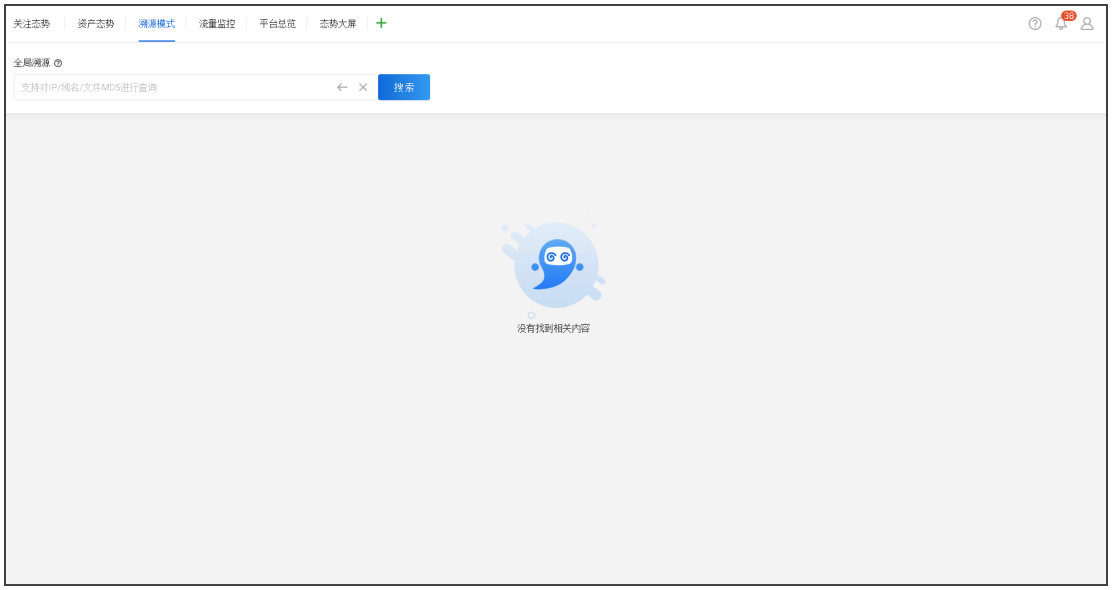
- 关联威胁事件方向分布：展示各方向的威胁事件数量。点击数字，系统将根据方向作为筛选条件筛选对应的威胁事件，并跳转至页面下方<威胁事件>标签页的威胁事件列表。
- 关联热点威胁资讯分布：展示各等级的和溯源对象相关的热点威胁资讯。点击数字，系统将根据等级作为筛选条件筛选对应的热点威胁资讯，并跳转至<关联热点资讯>标签页。

- **威胁事件**：展示指定时间内该溯源对象上发生的威胁事件详情。
  - <威胁事件>标签页：以列表的方式展示指定时间内该溯源对象上发生的已解决和未解决威胁事件。具体操作，请参阅事件列表部分。
  - <导致失陷威胁事件>标签页：展示资产评估时间前30天内，与该溯源对象关联的资产上的失陷威胁事件，默认展示源IP为服务器的导致失陷威胁事件。点击威胁事件名称，打开威胁事件详情页面，查看所选威胁事件的详细信息。
  - <威胁透视镜>标签页：以图标和箭头连接线的形式展示指定时间内该溯源对象上发生的威胁事件之间的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。点击指定的IP地址，查看该威胁事件的源、目的IP，以及与源、目的IP关联的威胁事件Top5。关联威胁事件Top5按照级别降序排列，级别相同的按照发生次数降序排列。
- **关联热点威胁资讯**：展示指定时间内和溯源对象相关的热点威胁资讯。
  - 点击右上角威胁级别按钮，筛选指定级别的威胁资讯。
  - 具体配置，请参阅热点威胁资讯部分。

- 点击 ← 按钮，回退到上一次的溯源页面。
- 点击 × 按钮，清除文本框中的内容。

无结果

若未搜索到指定对象相关的内容，页面中提示“没有找到相关内容”。



注意: 搜索威胁事件时仅支持搜索非误报事件，若搜索误报的威胁事件，则会显示“没有找到相关内容”。

流量监控

<流量监控>标签页中对智源平台获取的NetFlow数据信息从流量趋势、新建连接趋势、源IP活动、目的IP活动多方面进行统计和展示。

过滤条件



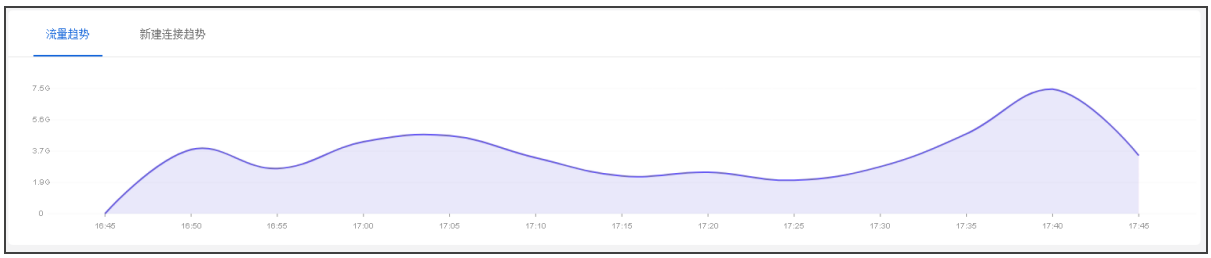
流量监控页面上方，可以指定过滤条件，来过滤该页面中数据的统计的范围，符合条件的数据将在下方其他统计图表中展示：

- 时间：指定统计的时间范围，可选择具体的开始时间和结束时间或者直接点击“1小时/12小时/24小时/7天/30天”进行过滤。
- 来源设备：指定统计数据的来源设备。

- 区域：指定统计数据的所属区域。
- 资产类型：指定统计数据对应的资产类型，终端、服务器或者非资产的其他设备。
- 源IP：指定统计数据的源IP地址类型和IP地址。
- 目的IP：指定统计数据的目的IP地址类型和IP地址。

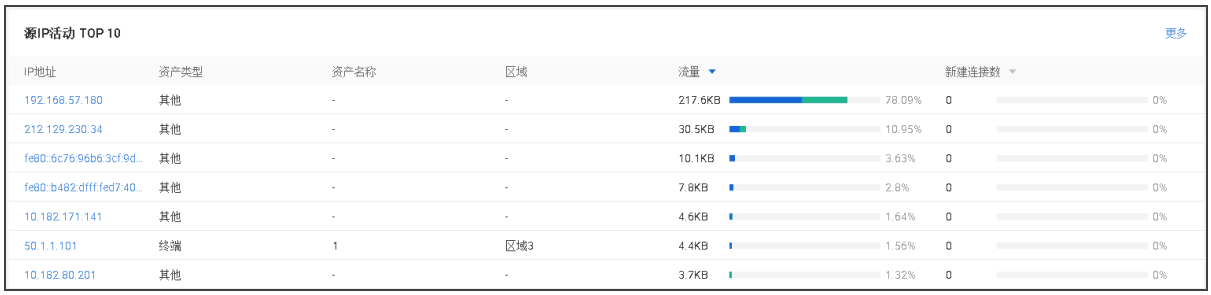
流量趋势

流量趋势标签页根据指定的过滤条件，以曲线图形式展示总流量的变化趋势或者新建连接变化趋势。



源IP活动 TOP 10

源IP活动TOP 10 部分根据指定的过滤条件，以列表形式展示总流量排名前10的源IP流量统计信息。



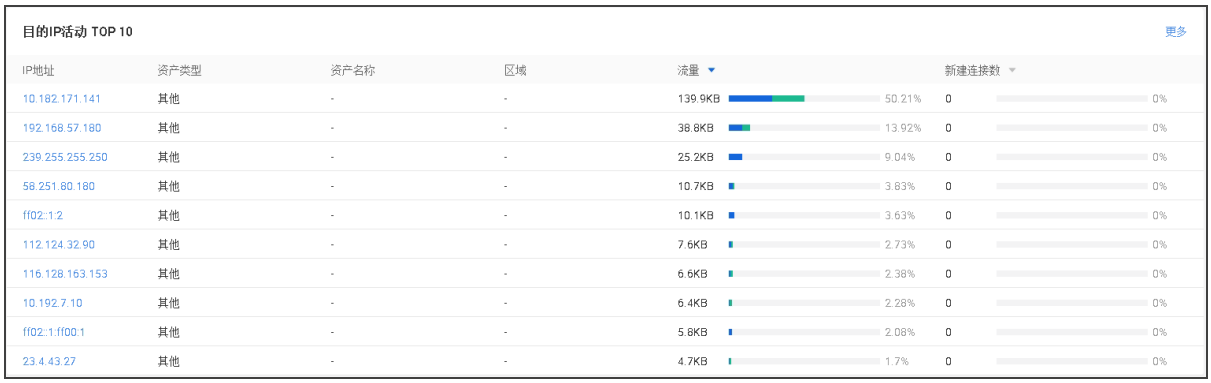
- 在列表“流量”或“新建连接数”列中点击 按钮，可指定列表中源IP流量统计信息按照总流量或新建连接数排名。
- 点击源IP地址链接，打开详情页面，查看以下详情内容：
  - 源IP基本信息：包括所选源IP地址对应的资产类型、资产名称、所属区域、新建连接数，以及上下行流量、总流量大小；
  - 协议流量分布：以柱状图形式展示总流量排名前5的协议流量统计信息；

- 流量趋势/新建连接趋势：以曲线图形式展示所选源IP的总流量的变化趋势或者新建连接变化趋势；
- 关联目的IP活动：以列表形式展示与所选源IP相关联的所有目的IP流量统计信息。

- 点击右上角“更多”，查看所有源IP流量统计信息。

目的IP活动 TOP 10

目的IP活动TOP 10 部分根据指定的过滤条件，以列表形式展示总流量排名前10的目的IP流量统计信息。

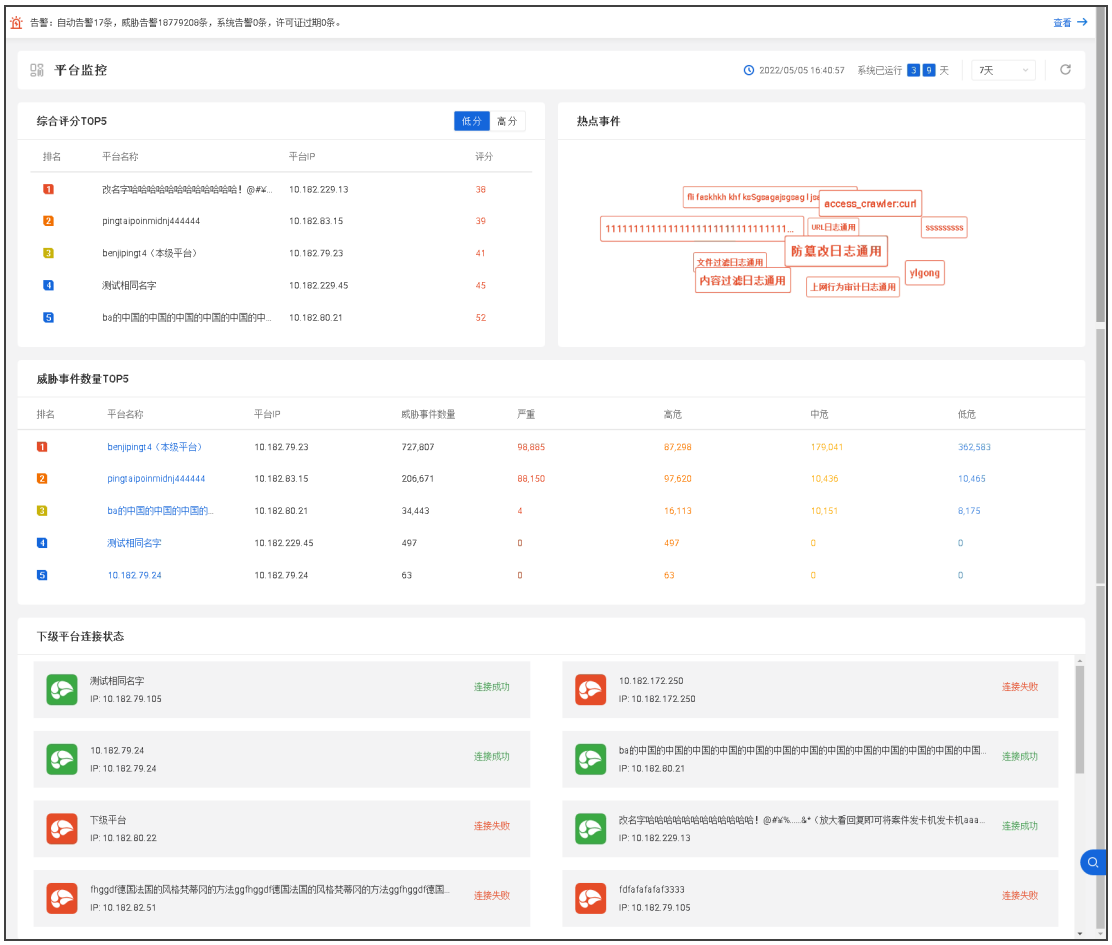


- 在列表“流量”或“新建连接数”列中点击 按钮，可指定列表中目的IP流量统计信息按照总流量或新建连接数排名。
- 点击目的IP地址链接，打开详情页面，查看以下详情内容：
  - 目的IP基本信息：包括所选目的IP地址对应的资产类型、资产名称、所属区域、新建连接数，以及上下行流量、总流量大小；
  - 协议流量分布：以柱状图形式展示总流量排名前5的协议流量统计信息；
  - 流量趋势/新建连接趋势：以曲线图形式展示所选目的IP的总流量的变化趋势或者新建连接变化趋势；
  - 关联源IP活动：以列表形式展示与所选目的IP相关联的所有源IP流量统计信息。
- 点击右上角“更多”，查看所有目的IP流量统计信息。

平台总览

仅当本平台为上级平台时支持展示该页面。

<平台总览>页面展示了本平台以及与本平台连接成功的下级平台中，综合评分TOP5和威胁事件数量TOP5的平台，以及平台中的热点事件，同时展示了各下级平台的连接状态。



- 右上角显示当前系统时间、系统运行时长。
- 点击 按钮，立即刷新<平台总览>页面的数据。
- 点击时间下拉框，选择数据统计的时间范围。系统支持选择“24小时”、“7天”或“30天”。默认情况下时间范围为7天。
- 综合评分TOP5

- 列表中展示综合评分排名前5的平台信息，包括“平台名称”、“平台IP”以及“评分”。
- 点击“低分”按钮，本级平台以及下级平台将按照评分从低到高排列，并在列表中展示排名前5的平台；点击“高分”按钮，本级平台以及下级平台将按照评分从高到低排列，并在列表中展示排名前5的平台。

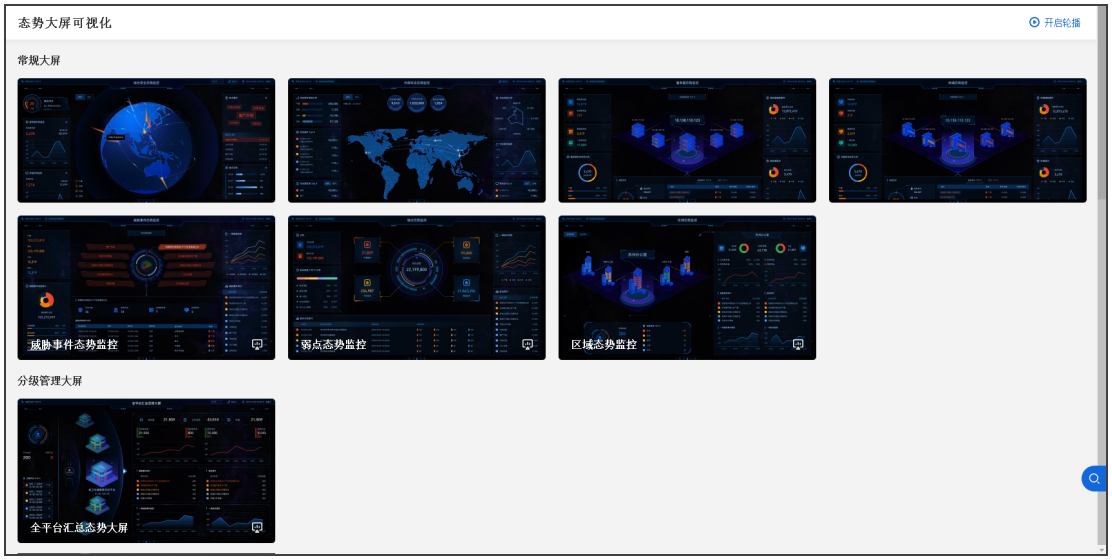
- 热点事件
  - 汇总指定时间内所有平台的已解决和未解决的威胁事件，并展示数量排名前10的事件。
  - 点击事件的名称，跳转至"事件列表" 在第136页页面，在<综合视角>标签页查看指定名称、指定时间内的已解决和未解决威胁事件信息，威胁事件按时间降序排列。

- 威胁事件数量TOP5
  - 列表中展示指定时间内已解决和未解决威胁事件数量排名前5的平台信息，包括“平台名称”、“平台IP”、“威胁事件数量”、“严重”等级威胁事件数量、“高危”等级威胁事件数量、“中危”等级威胁事件数量以及“低危”等级威胁事件数量。
  - 点击“平台名称”，跳转至"事件列表" 在第136页页面，在<综合视角>标签页查看指定平台、指定时间内已解决和未解决的威胁事件信息，威胁事件按时间降序排列。

- 下级平台连接状态
  - 列表中展示下级平台与本平台的连接状态，支持展示下级平台的名称、IP和连接状态。绿色代表连接成功，红色代表连接失败。

态势大屏

<态势大屏>标签页中展示了支持的大屏缩略图。



- 鼠标悬停在缩略图上，可以查看大屏的简介。包括“常规大屏”部分和“分级管理大屏”部分，所有的设备上均包含“常规大屏”部分，“分级管理大屏”部分仅有被设为上级平台的设备支持展示。
- 若本平台为上级平台，点击大屏左上角下拉框，可以切换至任意在线的下级平台，查看不同平台的态势监控。默认情况下显示为本级平台的态势监控。
- 点击“开启轮播”，在新的页面打开态势大屏，设备上所有的大屏以一定的时间开始轮播。用户可以在大屏页面自定义每张大屏停留的时间，可配置的范围为10到120秒，系统默认为60秒。若切换至其他平台，则会轮播指定平台的态势大屏。若轮播中途平台离线，则大屏中会显示空数据。
- 点击缩略图，在新的页面打开指定的大屏。投屏模式页面中支持展示“今天”、“近7天”或“近30天”内的数据信息。为了保证投屏监控模式页面正常显示，请将投屏的电脑分辨率设置为1920*1080。
  - 常规大屏：所有平台均包含全部常规大屏。



- 综合安全态势监控展示综合评分，全球威胁实时监控、资产态势、热点事件、弱点态势、威胁事件等综合信息。



- 外部攻击态势监控展示攻击事件等级分布、全球攻击实时监控、攻击源IP TOP5、攻击源地理位置TOP5、攻击阶段分布、攻击事件态势、受攻击TOP5等态势信息。



- 服务器态势监控展示风险服务器、服务器安全状态分布、风险服务器状态、服务器威胁事件、服务器弱点等态势信息。



- 终端态势监控展示风险终端、终端安全状态分布、风险终端状态、终端威胁事件、终端弱点等态势信息。

- 

威胁事件态势监控展示事件威胁等级分布、威胁事件类型统计、威胁事件详情轮播、威胁态势、威胁事件排行等态势信息。

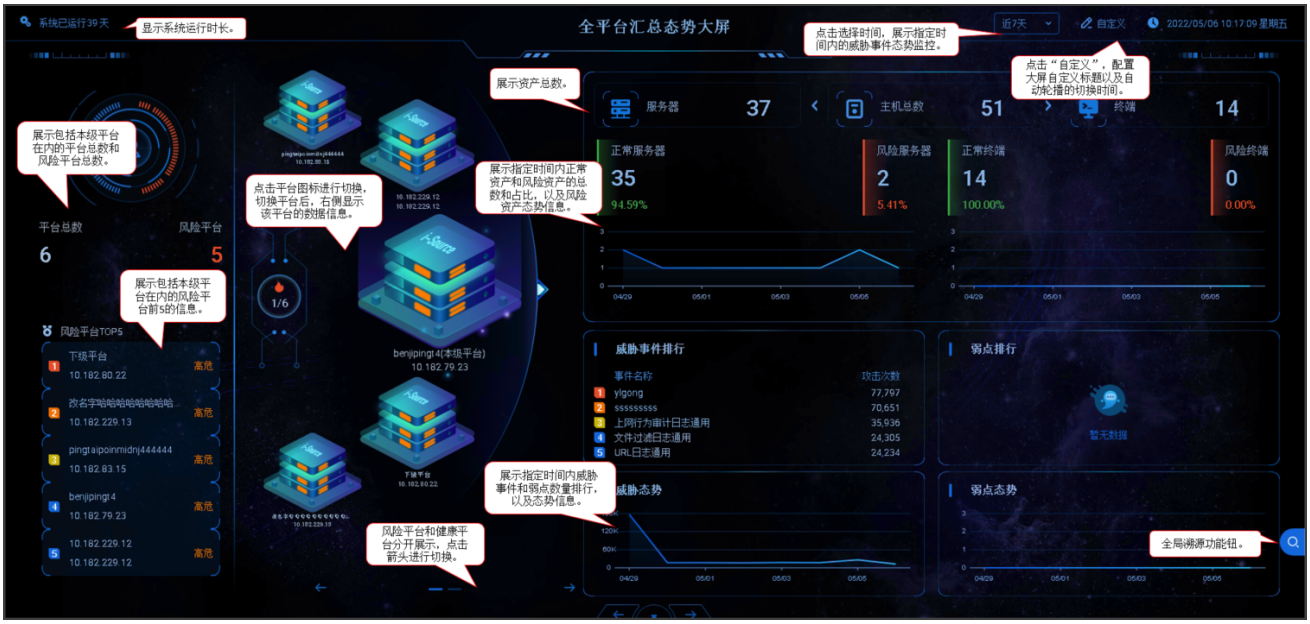
- 

弱点态势监控展示弱点主机数目占比、弱点等级占比、弱点类型TOP5分布、弱点主机排行、弱点态势、弱点排行等弱点信息。



- 区域态势监控展示各个区域数目及详情、风险区域TOP5、各个区域的威胁事件、资产弱点、风险资产等信息。

- 分级管理大屏：仅有上级平台支持该类型的大屏。

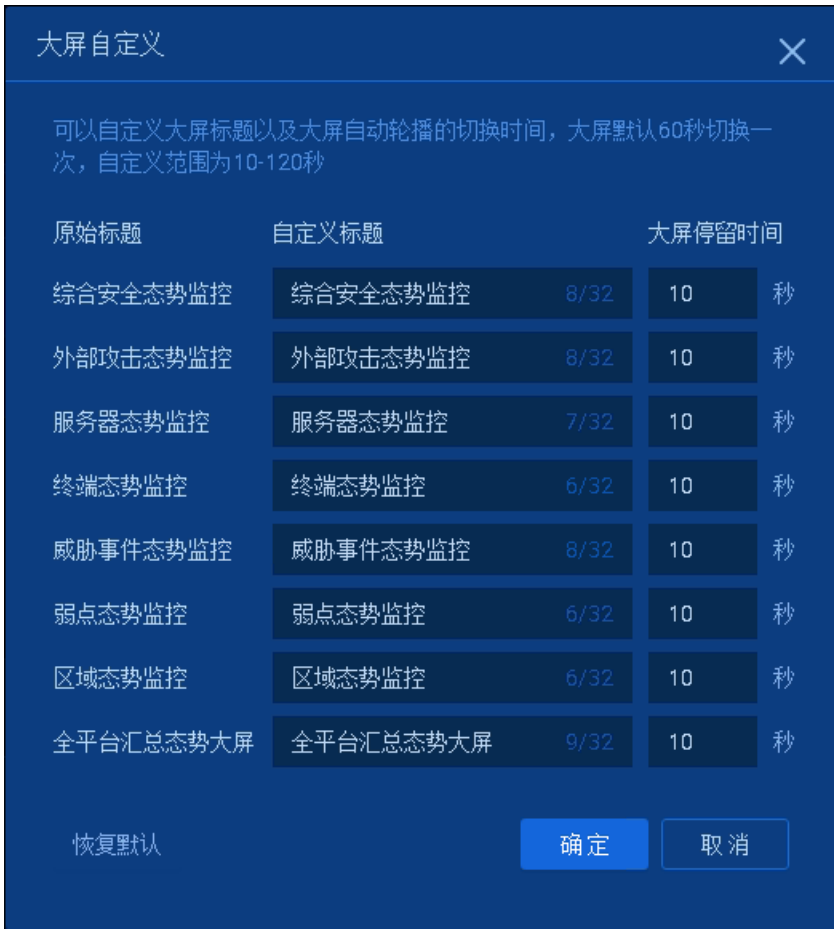


- 全平台汇总态势大屏展示全平台风险态势、本级及下级平台的威胁事件、风险资产等相关信息。

投屏模式自定义配置

用户可以自定义态势监控的投屏模式的标题以及各大屏自动轮播的切换时间。

进入投屏模式后，点击右上角“自定义”按钮，打开<大屏自定义>对话框。



- 在“自定义标题”文本框中配置自定义大屏标题，范围是0-32个字符。如未配置，则显示为默认的原始标题。
- 在“大屏停留时间”处指定各大屏自动轮播的切换时间，范围是10-120秒，默认情况下，大屏自动轮播时间为60秒。
- 点击“恢复默认”将恢复为原始标题以及60秒切换一次大屏页面。

自定义模块

<自定义模块>标签页可以自定义创建模块，获取用户关心的数据内容。

自定义模块配置包括：

1. 创建自定义模块。 当前系统最多可配置4个自定义模块。
2. 添加看板：在自定义模块中，添加看板，以将用户关注的数据信息添加到自定义模块中。一个自定义模块里可以最多添加9个看板。
3. 修改/删除看板：在看板页面的右上角，点击“ ”编辑或删除看板内容。
4. 放大/缩小看板：在看板页面的右上角，点击“ ”并拖拽看板，可对其进行放大或缩小。
5. 重命名自定义模块：在态势监控页面，选择自定义模块的名称并点击其后的“ ”，在弹出的下拉菜单中，选择“重命名”。
6. 删除自定义模块：在态势监控页面，选择自定义模块的名称并点击其后的“ ”，在弹出的下拉菜单中，选择“删除”。
7. 将自定义模块设置为默认模块。

新建自定义模块

新建自定义模块，请按照以下步骤进行操作：

1. 点击“态势监控”。
2. 点击页面左上角“总览”右侧的“+”按钮，在弹出的文本框中输入模块的名称，并点击“ ”。自定义名称最多允许输入12个字符。



3. 系统将进入到新建的自定义模块标签页中。在该页面，用户需添加看板，以将自己感兴趣的内容展示在该模块中。

4. 点击“新看板”上方的“+”或点击 新看板，弹出<新看板>页面。



填写看板配置的相关参数。

选项	说明
标题	输入看板的标题，如“一周风险监控”。
展示内容	选择需要展示的内容，可选“资产”、“威胁”或“弱点”对应的可展示内容。
图表类型	选择展示的图表类型。根据“展示内容”的不同，图表类型不同。
时间	选择需要统计的时间。
区域	选择需要统计的区域。请先在<区域管理>页面配置区域，具

选项	说明
	体请参见区域管理一节。

5. 点击“确定”完成配置。

例：添加看板

例如，某企业管理员想要统计“一周内苏州区域的Top威胁事件”信息，并以图表形式展示。在新建看板时，参考如下信息：



设置为默认模块

用户可将已创建的自定义模块，设置为默认模块。设置后，当进入“态势监控”页面时，将直接进入该默认模块，而不是“总览”页面。请按以下步骤进行操作：

1. 点击“态势监控”。

2. 选择需要设置为默认的自定义模块名称，点击其后的“ ”，在弹出的下拉菜单中，选择“设为默认”。



用户可使用以上操作方式，在下拉菜单中选择“取消默认”，该自定义模块将不再是默认模块。进入“态势监控”页面时，将直接进入“总览”页面。

多标签页展示

系统支持多标签页展示页面，当用户需要同时查看多个功能模块的页面时，可以通过“Ctrl键+鼠标左键点击一级菜单”的方式，即可打开对应所选一级菜单的新标签页。

第3章 威胁分析

威胁分析页面提供多维度、深层次的威胁和日志信息的展现和检索功能，以图例或表格的方式展示通过威胁/攻击链规则检测出的威胁事件、风险资产（存在未解决威胁事件的服务器或终端）以及业务相关数据，并且展示了采集的所有日志信息（来自于山石网科安全设备、流量探针、威胁探针、Linux系统设备和用户主机），方便用户查看和检索。

威胁分析部分包含如下内容：

- "威胁" 在第115页：介绍如何查看和检索指定时间段和区域的威胁事件、风险资产以及业务信息，包括风险级别、数量、变化趋势等。
- "日志" 在第146页：介绍如何查看和检索指定时间段的日志信息，包括Syslog、NetFlow、Meta Data、Sysmon以及Linux五种类型。

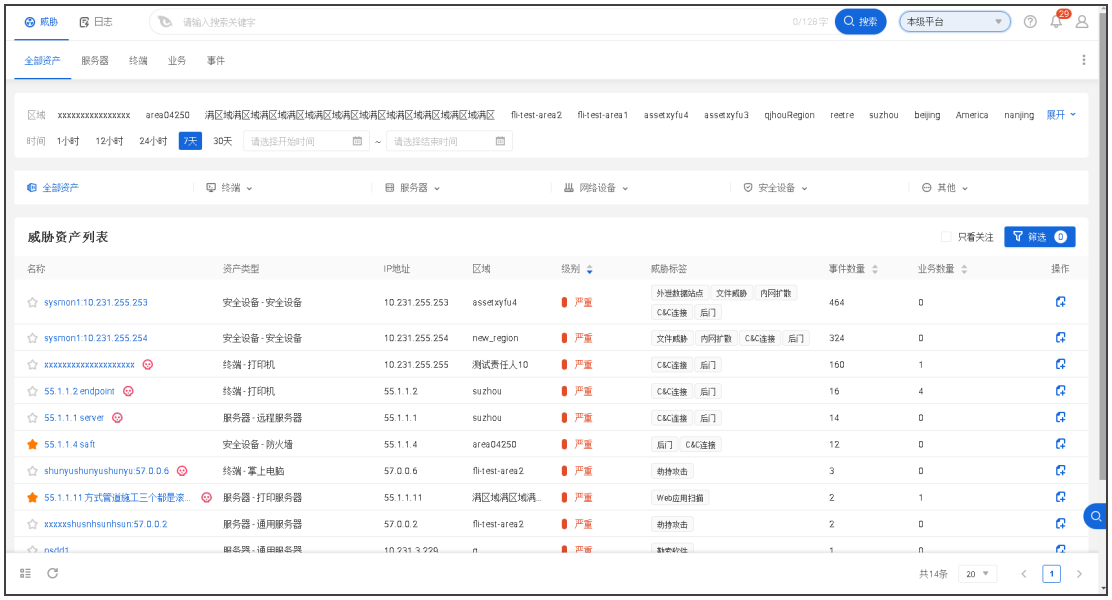
威胁

以表格等方式展示指定时间段和区域的威胁事件、风险资产以及业务信息，包括风险级别、数量等，方便用户查看和检索。

点击右上角 按钮，展开页签。点击页签前的 按钮，收藏该页签。收藏后，点击“威胁分析”时将首先展示收藏的页签。仅支持收藏一个页签，默认为“全部资产”页签。

全部资产

全部资产列表展示了系统中所有威胁资产相关信息。点击“威胁分析”，打开威胁页面，点击<全部资产>标签页。

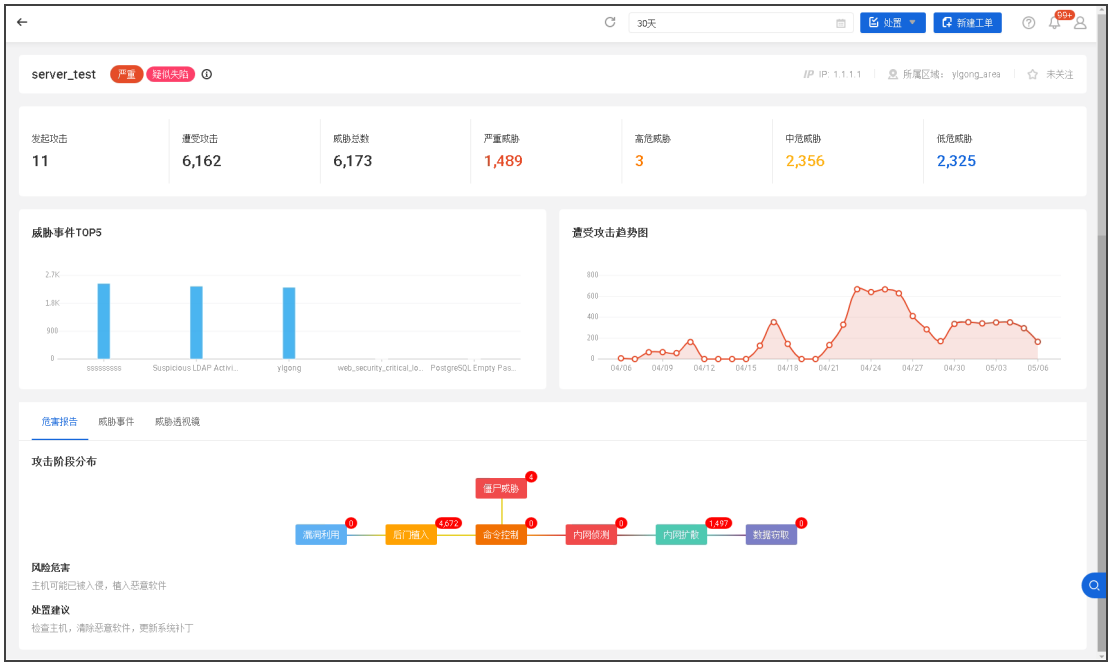


- 点击上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的威胁资产信息显示在威胁资产列表中。
- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的全部资产信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的资产信息。当选择下级平台时，仅支持查看资产信息，不支持新建工单的操作。
- 选择威胁资产所在的区域、资产种类以及威胁事件发生的时间范围，符合条件的威胁资产信息将展示在列表中。默认的时间范围为7天。

    - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
    - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击列表上方  按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的资产信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
    - 点击列表中具体资产前的 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”复选框，列表中将展示被设为重点关注的威胁资产。
- 威胁资产的默认排序规则是按照“级别”进行降序。点击表头中“级别”、“事件数量”或“业务数量”后的  按钮，可将威胁资产进行重新排序：
    - 点击对应按钮后，当按钮显示为  时，将威胁资产按照“级别”、“事件数量”或“业务数量”进行降序排列。
    - 点击对应按钮后，当按钮显示为  时，将威胁资产按照“级别”、“事件数量”或“业务数量”进行升序排列。
    - 当“级别”、“事件数量”和“业务数量”后的按钮同时显示为  时，将威胁资产进行随机排列。
- 点击列表中的“名称”链接，查看所选威胁资产的详细信息。
- 点击列表中的  按钮，在打开的页面中新建工单，从而对威胁资产进行响应，并且通知到指定处理人实施人工处理。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新威胁资产列表。

查看资产详细信息

在详细信息页面，可以查看所选资产的概览信息、威胁事件TOP5、遭受攻击趋势图、危害报告、威胁事件以及威胁透视镜。



- 概览：展示所选资产在指定时间内发起攻击的次数、遭受攻击的次数、威胁事件总数，以及各级别威胁事件的数量。
    - 点击发起攻击对应的数字，系统将根据源IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击威胁总数对应的数字，系统将根据“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- 威胁事件TOP5：以柱状图形式展示所选资产指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。

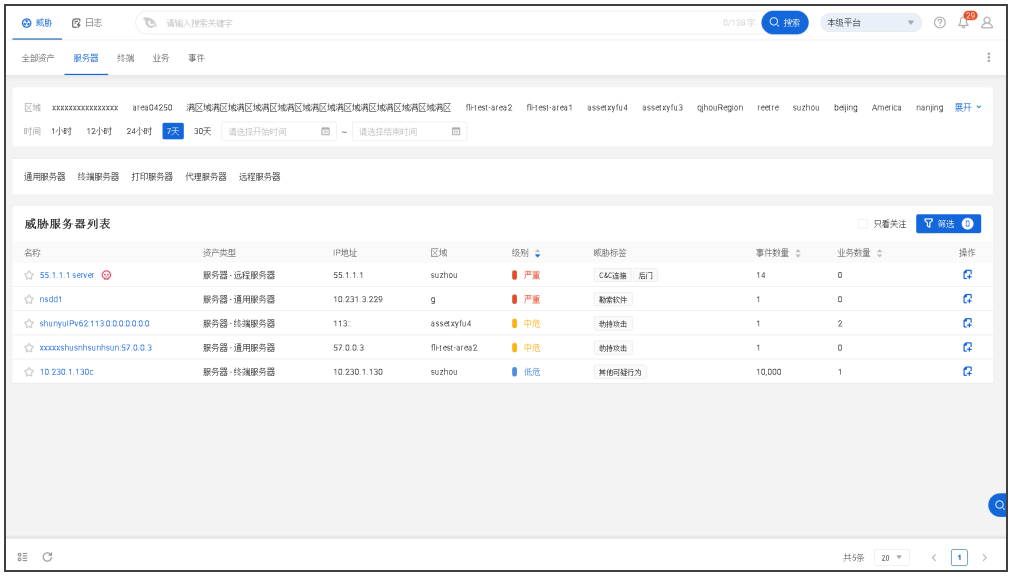
- 遭受攻击趋势图：以曲线图的方式展示所选资产指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选资产发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内所选资产发生的威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示关注的威胁事件。
- **威胁透视镜**：以图标和箭头连接线的形式展示指定时间周期内所选资产发生的威胁事件的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。
    - 点击上方

按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 页面右上角的时间与威胁资产列表上方的时间保持一致。若需查看所选威胁资产在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。
- **处置**：点击下拉菜单选择处置动作，针对所选威胁资产配置响应的处置动作，下发至指定的联动实体对风险进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该资产不是本级平台的资产，则不支持配置处置动作。
- 点击页面右上角的

按钮，在打开的页面中新建工单，从而对所选威胁资产进行响应，并且通知到指定处理人实施人工处理。若该资产不是本级平台的资产，则不支持新建工单。
- 点击页面右上角的按钮，刷新页面的统计显示。

服务器列表

服务器列表页面统计并展示所有风险服务器相关信息。点击“威胁分析”，打开威胁页面，点击<服务器>标签页。



- 点击上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的服务器信息显示在服务器列表中。
- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的服务器信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的服务器信息。当选择下级平台时，仅支持查看服务器信息，不支持新建工单的操作。
- 选择威胁服务器所在的区域、服务器子类以及威胁事件发生的时间范围，符合条件的服务器信息将展示在列表中。默认的时间范围为7天。
    - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
    - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击列表上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的服务器信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
    - 点击列表中具体资产前的 ☆ 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”复选框，列表中将展示被设为重点关注的风险服务器。

- 服务器的默认排序规则是按照“级别”进行降序。点击表头中“级别”、“事件数量”或“业务数量”后的 按钮，可将服务器进行重新排序：
  - 点击对应按钮后，当按钮显示为 时，将服务器按照“级别”、“事件数量”或“业务数量”进行降序排列。
  - 点击对应按钮后，当按钮显示为 时，将服务器按照“级别”、“事件数量”或“业务数量”进行升序排列。
  - 当“级别”、“事件数量”和“业务数量”后的按钮同时显示为 时，将服务器进行随机排列。
- 点击列表中的“名称”链接，查看所选服务器的详细信息。
- 点击列表中的 按钮，在打开的页面中新建工单，从而对风险服务器进行响应，并且通知到指定处理人实施人工处理。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新服务器列表。

查看服务器详细信息

在详细信息页面，可以查看所选服务器的概览信息、威胁事件TOP5、遭受攻击趋势图、危害报告、威胁事件以及威胁透视镜。



- 概览：展示所选服务器在指定时间内发起攻击的次数、遭受攻击的次数、威胁事件总数，以及各级别威胁事件的数量。
    - 点击发起攻击对应的数字，系统将根据源IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击威胁总数对应的数字，系统将根据“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- 威胁事件TOP5：以柱状图形式展示所选服务器指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- 遭受攻击趋势图：以曲线图的方式展示所选服务器指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选服务器发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。

- **威胁事件**：以列表的方式展示指定时间周期内所选服务器发生的威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示关注的威胁事件。
- **威胁透视镜**：以图标和箭头连接线的形式展示指定时间周期内所选服务器发生的威胁事件的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。
  - 点击上方 

按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 页面右上角的时间与风险服务器列表上方的时间保持一致。若需查看所选风险服务器在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。
- **处置**：点击下拉菜单选择处置动作，针对所选风险服务器配置响应的处置动作，下发至指定的联动实体对风险进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该服务器不是本级平台的服务器，则不支持配置处置动作。
- 点击页面右上角的 

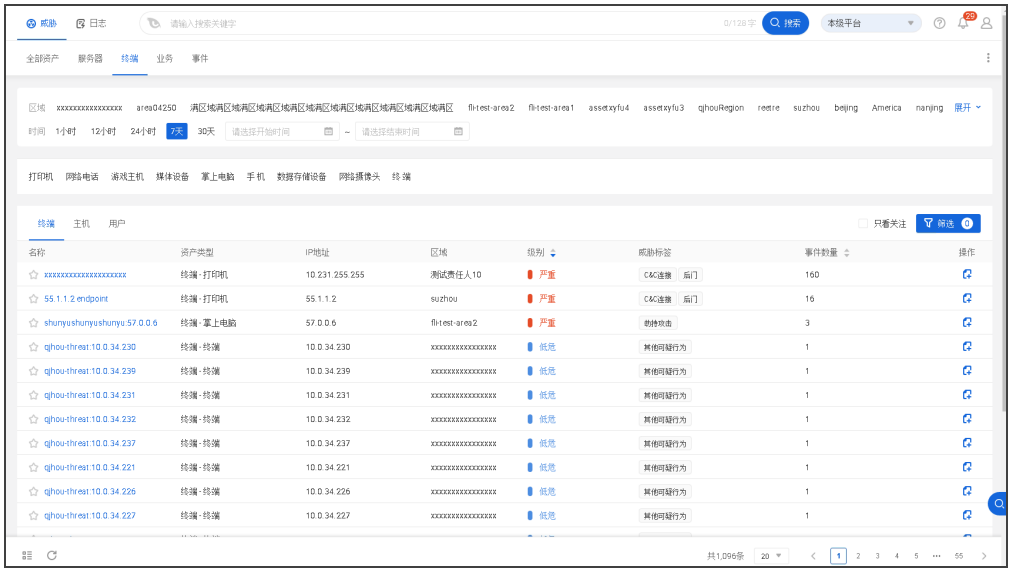
按钮，在打开的页面中新建工单，从而对所选风险服务器进行响应，并且通知到指定处理人实施人工处理。若该服务器不是本级平台的服务器，则不支持新建工单。
- 点击页面右上角的  按钮，刷新页面的统计显示。

终端

终端、主机和用户标签页分别从IP地址、设备（mac地址）和用户名的角度，统计接入网络的终端信息，包括级别、威胁标签和威胁数量等。其中，主机的mac地址和用户的用户名是从第三方认证服务器（深澜认证计费系统Srun4000）发送的认证计费报文中提取的。

终端列表

点击“威胁分析 > 终端 > 终端”打开终端列表页面。



- 点击上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的终端信息显示在终端列表中。
- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的终端信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的终端信息。当选择下级平台时，仅支持查看终端信息，不支持新建工单的操作。
- 选择终端所在的区域、终端子类以及威胁事件发生的时间范围，符合条件的终端信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击列表上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的终端信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
  - 点击列表中具体资产前的 ☆ 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”复选框，列表中将展示被设为重点关注的终端。

- 终端的默认排序规则是按照“级别”进行降序。点击表头中“级别”或“事件数量”后的 按钮，可将终端进行重新排序：
  - 点击对应按钮后，当按钮显示为 时，将终端按照“级别”或“事件数量”进行降序排列。
  - 点击对应按钮后，当按钮显示为 时，将终端按照“级别”或“事件数量”进行升序排列。
  - 当“级别”和“事件数量”后的按钮同时显示为 时，将终端进行随机排列。
- 点击列表中的“名称”链接，查看所选终端的详细信息。
- 点击列表中的 按钮，在弹出对话框中新建工单，从而对所选风险终端进行响应，并且通知到指定处理人实施人工处理。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新终端列表。

查看终端详细信息

在详细信息页面，可以查看所选终端的概览信息、威胁事件TOP5、遭受攻击趋势图、危害报告、威胁事件以及威胁透视镜。



- 概览：展示所选终端发起攻击的次数、被攻击的次数、发生的威胁事件总数，以及各级别威胁事件的数量。
    - 点击发起攻击对应的数字，系统将根据源IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击威胁总数对应的数字，系统将根据“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- 威胁事件TOP5：以柱状图形式展示所选终端指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- 遭受攻击趋势图：以曲线图的方式展示所选终端指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点的被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选终端发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。

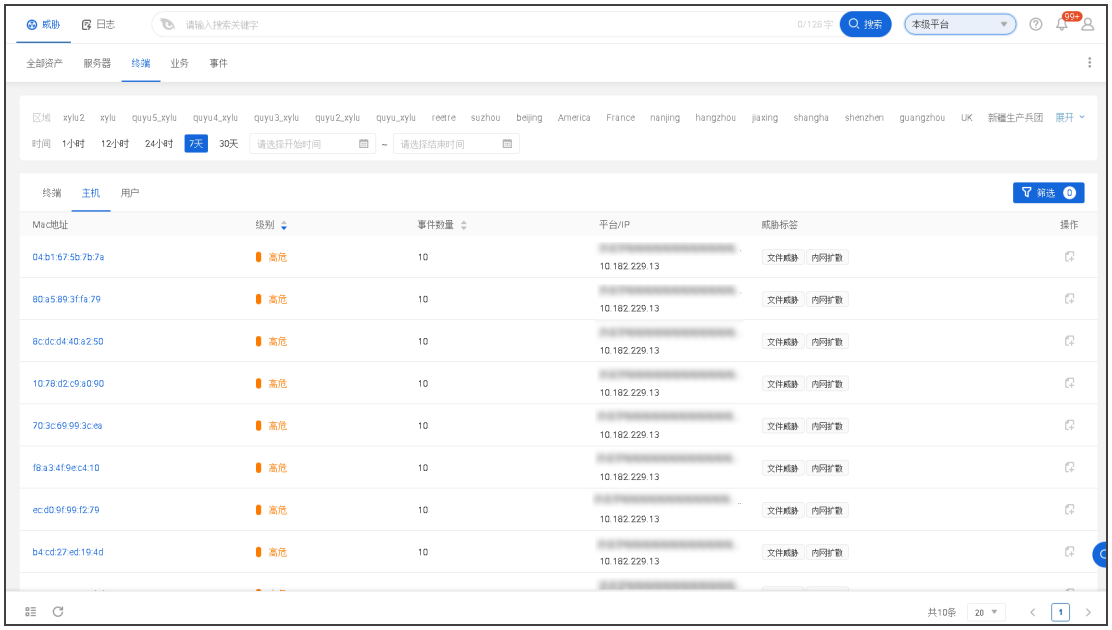
- **威胁事件**：以列表的方式展示指定时间周期内所选终端发生的威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示关注的威胁事件。
- **威胁透视镜**：以图标和箭头连接线的形式展示指定时间周期内所选终端发生的威胁事件的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。
  - 点击上方 

按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 页面右上角的时间与终端列表上方的时间保持一致。若需查看所选终端在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。
- **处置**：点击下拉菜单选择处置动作，针对所选风险终端配置响应的处置动作，下发至指定的联动实体对风险进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该终端不是本级平台的终端，则不支持配置处置动作。
- 点击页面右上角的 

按钮，在弹出对话框中新建工单，从而对风险终端进行响应，并且通知到指定处理人实施人工处理。若该终端不是本级平台的终端，则不支持新建工单。
- 点击页面右上角的  按钮，刷新页面的统计显示。

主机列表

点击“威胁分析 > 终端 > 主机”打开主机列表页面。



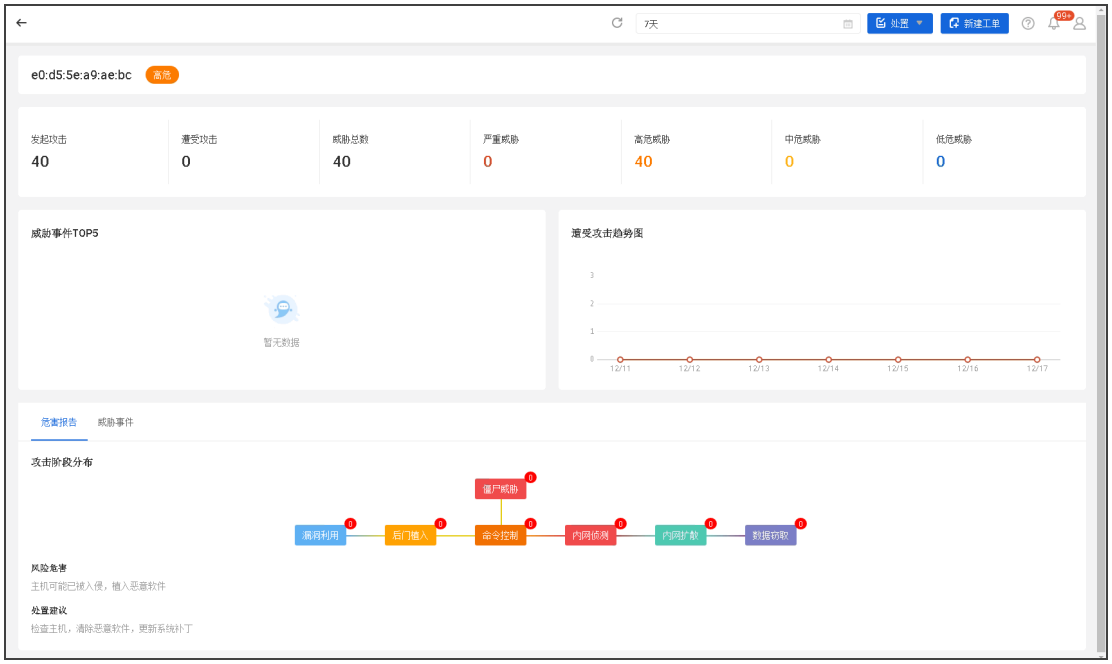
- 点击上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的主机信息显示在主机列表中。
- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的主机信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的主机信息。当选择下级平台时，仅支持查看主机信息，不支持新建工单的操作。
- 选择威胁事件发生的时间范围，符合条件的主机信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击列表上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的主机信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 主机的默认排序规则是按照“级别”进行降序。点击表头中“级别”或“威胁数量”后的 按钮，可将主机进行重新排序：

- 点击对应按钮后，当按钮显示为 时，将主机按照“级别”或“威胁数量”进行降序排列。
- 点击对应按钮后，当按钮显示为 时，将主机按照“级别”或“威胁数量”进行升序排列。
- 当“级别”和“威胁数量”后的按钮同时显示为 时，将主机进行随机排列。

- 点击列表中的“Mac地址”链接，查看所选主机的详细信息。
- 点击列表中的 按钮，在弹出对话框中新建工单，从而对所选主机进行响应，并且通知到指定处理人实施人工处理。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新主机列表。

查看主机详细信息

在详细信息页面，可以查看所选主机的概览信息、威胁事件TOP5、遭受攻击趋势图、危害报告以及威胁事件。



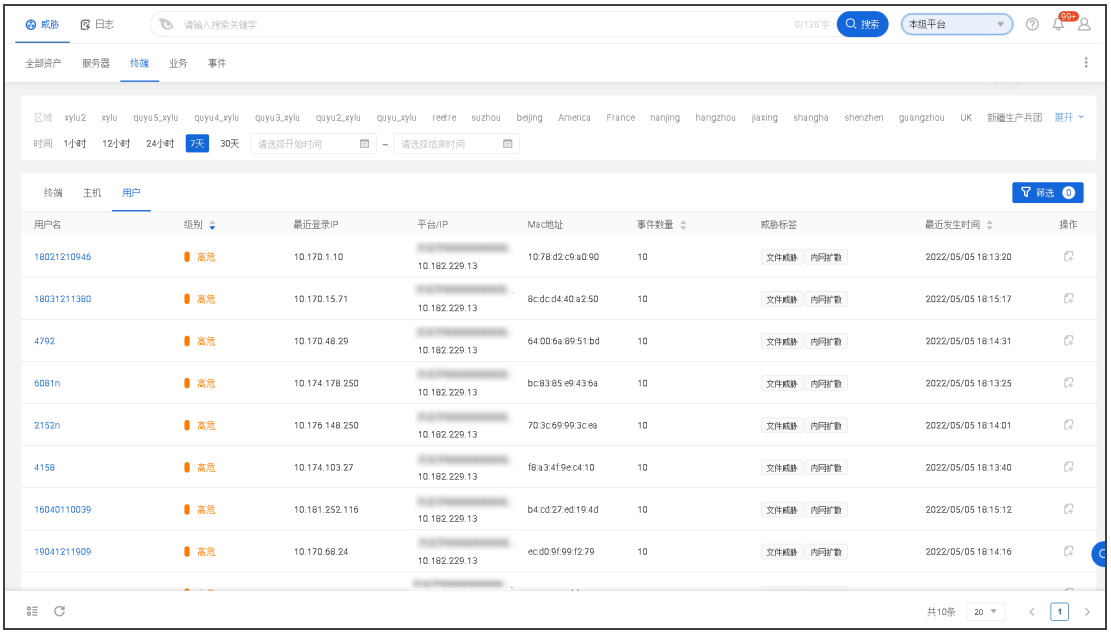
- 概览：展示所选主机发起攻击的次数、被攻击的次数、发生的威胁事件总数，以及各级别威胁事件的数量。
    - 点击发起攻击对应的数字，系统将根据源IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击威胁总数对应的数字，系统将根据“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- 威胁事件TOP5：以柱状图形式展示所选主机指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- 遭受攻击趋势图：以曲线图的方式展示所选主机指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点的被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选主机发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内所选主机发生的威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示关注的威胁事件。
- 页面右上角的时间与主机列表上方的时间保持一致。若需查看所选主机在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。
- **处置**：点击下拉菜单选择处置动作，针对所选主机配置响应的处置动作，下发至指定的联动实体对主机的风险进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该主机不是本级平台的主机，则不支持配置处置动作。

- 点击页面右上角的

按钮，在弹出对话框中新建工单，从而对风险主机进行响应，并且通知到指定处理人实施人工处理。若该主机不是本级平台的主机，则不支持新建工单。
- 点击页面右上角的按钮，刷新页面的统计显示。

用户列表

点击“威胁分析 > 终端 > 用户”打开用户列表页面。



- 点击上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的用户信息显示在用户列表中。
- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的用户信息。点击右上角

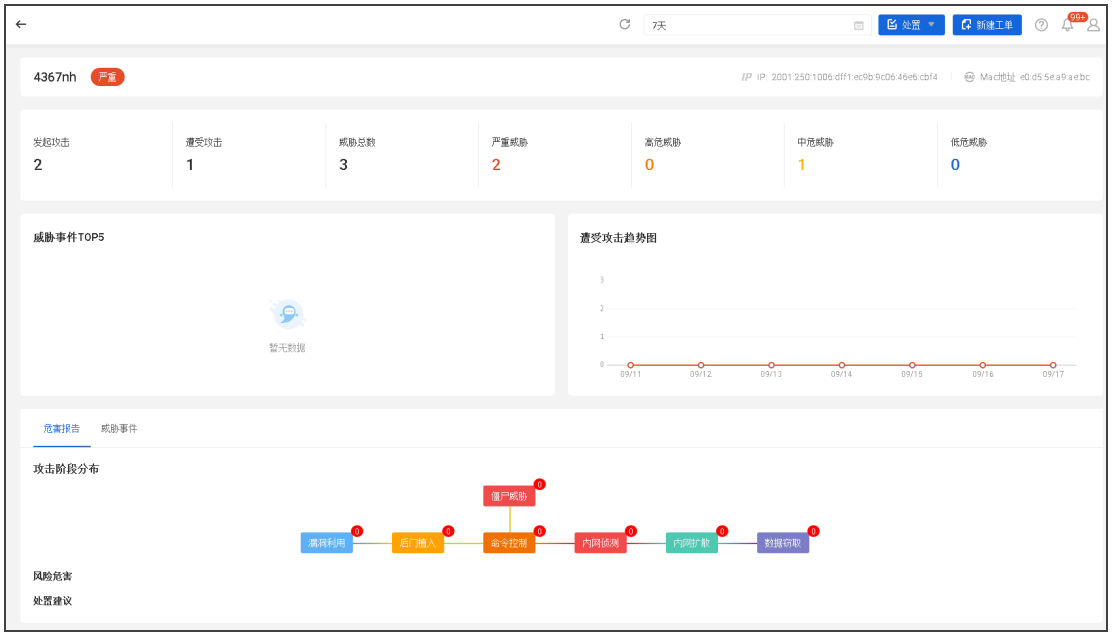
下拉框，选择查看的平台，下方列表中将展示指定平台的用户信息。当选择下级平台时，仅支持查看用户信息，不支持新建工单的操作。
- 选择威胁事件发生的时间范围，符合条件的用户信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。

- 点击列表上方 

按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的用户信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 用户的默认排序规则是按照“级别”进行降序。点击表头中“级别”、“威胁数量”或“最近发生时间”后的  按钮，可将用户进行重新排序：
  - 点击对应按钮后，当按钮显示为  时，将用户按照“级别”、“威胁数量”或“最近发生时间”进行降序排列。
  - 点击对应按钮后，当按钮显示为  时，将用户按照“级别”、“威胁数量”或“最近发生时间”进行升序排列。
  - 当“级别”、“威胁数量”或“最近发生时间”后的按钮同时显示为  时，将用户进行随机排列。
- 点击列表中的“用户名”链接，查看所选用户的详细信息。
- 列表中“IP地址”或“MAC地址”列显示用户的IP地址或MAC地址，方便进行溯源以及查看用户身份信息。
- 点击列表中的  按钮，在弹出对话框中新建工单，从而对所选用户进行响应，并且通知到指定处理人实施人工处理。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新用户列表。

查看用户详细信息

在详细信息页面，可以查看所选用户的身份信息、概览信息、威胁事件TOP5、遭受攻击趋势图、危害报告以及威胁事件。

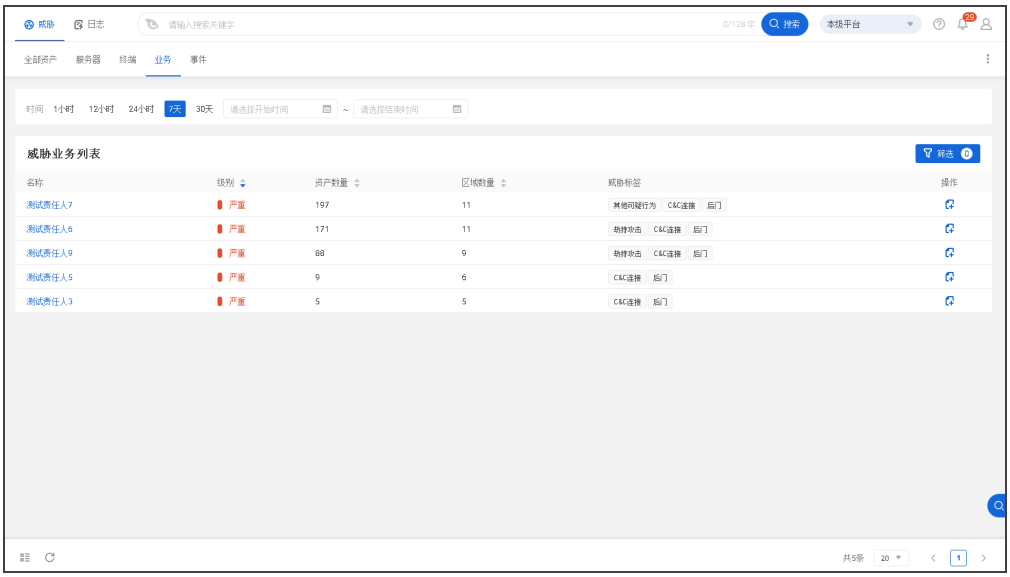


- 身份信息：展示所选用户的用户名、威胁级别、IP地址以及MAC地址。
- 概览：展示所选用户发起攻击的次数、被攻击的次数、发生的威胁事件总数，以及各级别威胁事件的数量。
    - 点击发起攻击对应的数字，系统将根据源IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击遭受攻击对应的数字，系统将根据目的IP地址和“未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击威胁总数对应的数字，系统将根据未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和未解决”状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- 威胁事件TOP5：以柱状图形式展示所选用户指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- 遭受攻击趋势图：以曲线图的方式展示所选用户指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点的被攻击的威胁事件的数量。

- **危害报告**：展示指定时间周期内所选用户发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内所选用户发生的威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注“复选框，列表中将展示关注的威胁事件。
- 页面右上角的时间与用户列表上方的时间保持一致。若需查看所选用户在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。
- **处置**：点击下拉菜单选择处置动作，针对所选用户配置响应的处置动作，下发至指定的联动实体对用户的风险进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该用户不是本级平台的用户，则不支持配置处置动作。
- 点击页面右上角的 新建工单 按钮，在弹出对话框中新建工单，从而对用户进行响应，并且通知到指定处理人实施人工处理。若该用户不是本级平台的用户，则不支持新建工单。
- 点击页面右上角的按钮，刷新页面的统计显示。

业务列表

业务列表页面统计并展示所有风险服务器上运行的业务信息。点击“威胁分析”，打开威胁页面，点击<业务>标签页。



- 点击上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的业务信息显示在业务列表中。
- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的业务信息。点击右上角 

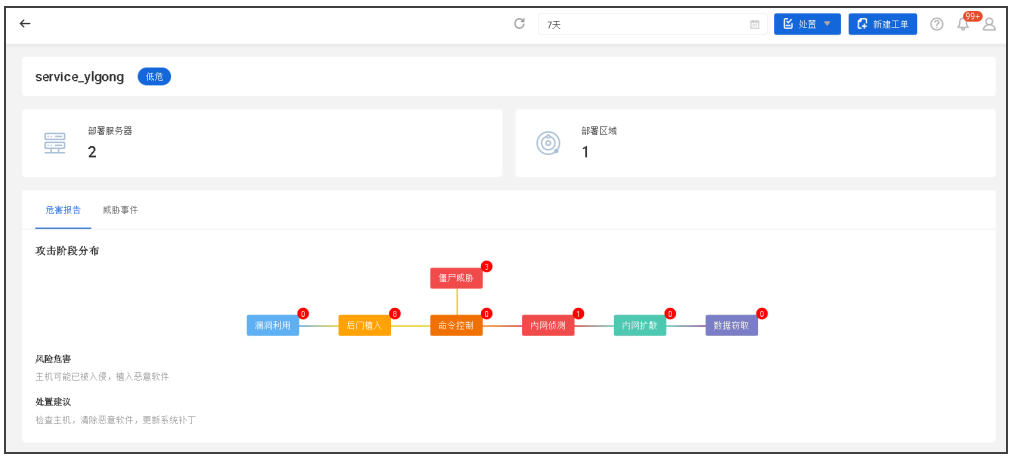
下拉框，选择查看的平台，下方列表中将展示指定平台的业务信息。当选择下级平台时，仅支持查看业务信息，不支持新建工单的操作。
- 选择业务中威胁事件发生的时间范围，符合条件的业务信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击列表上方 

按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的业务信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 业务的默认排序规则是按照“级别”进行降序。点击表头中“级别”、“服务器数量”或“区域数量”后的  按钮，可将业务进行重新排序：
  - 点击对应按钮后，当按钮显示为  时，将业务按照“级别”、“服务器数量”或“区域数量”进行降序排列。
  - 点击对应按钮后，当按钮显示为  时，将业务按照“级别”、“服务器数量”或“区域数量”进行升序排列。
  - 当“级别”、“服务器数量”和“区域数量”后的按钮同时显示为  时，将业务进行随机排列。
- 点击列表中的“名称”链接，查看所选业务的详细信息。
- 点击列表中的  按钮，在弹出对话框中新建工单，从而对运行指定业务的风险服务器进行响应，并且通知到指定处理人实施人工处理。

- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新业务列表。

查看业务详细信息

在详细信息页面，可以查看所选业务的描述信息、部署服务器和区域数量、危害报告以及威胁事件。



- **危害报告**：展示指定时间周期内（最近1小时、最近2小时、最近24小时、最近3天、最近7天、最近30天）业务所在服务器发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内（最近1小时、最近2小时、最近24小时、最近3天、最近7天、最近30天）业务所在服务器发生的威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示关注的威胁事件。
- 页面右上角的时间与业务列表上方的时间保持一致。若需查看所选业务在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。
- **处置**：点击下拉菜单选择处置动作，针对所选业务配置响应的处置动作，下发至指定的联动实体对业务的风险进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该业务不是本级平台的业务，则不支持配置处置动作。

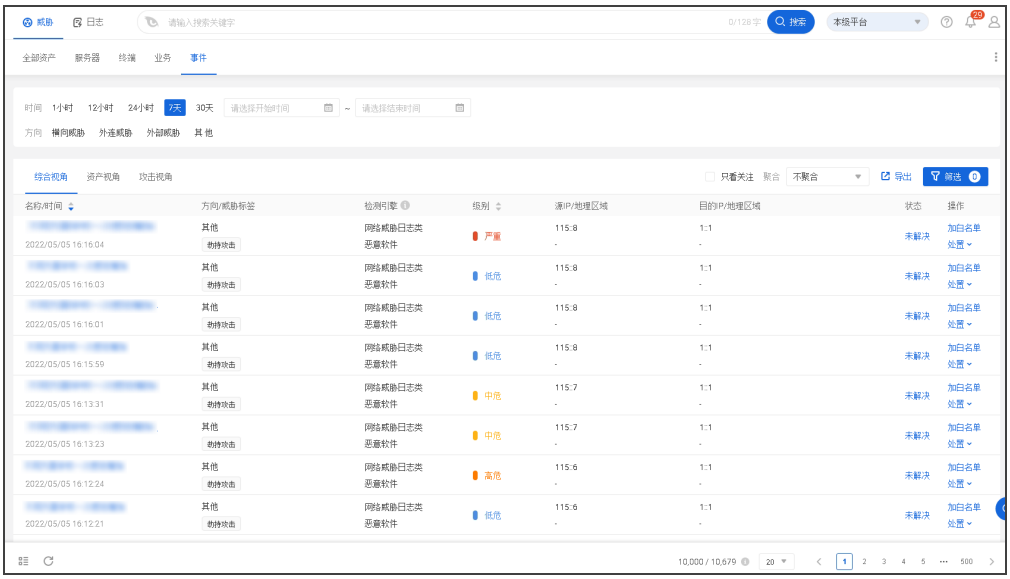
- 点击页面右上角的

按钮，在弹出对话框中新建工单，从而对运行指定业务的风险服务器进行响应，并且通知到指定处理人实施人工处理。若该业务不是本级平台的业务，则不支持新建工单。

- 点击页面右上角的按钮，刷新页面的统计显示。

事件列表

事件列表页面统计并展示指定方向或时间段内，由于匹配威胁规则而产生的所有威胁事件信息。点击“威胁分析”，打开威胁页面，点击<事件>标签页，打开事件列表页面。



- 点击上方的“请输入搜索关键字”文本框，自动展开推荐关键字和历史记录。点击历史记录、推荐关键字或直接输入关键字，然后点击“搜索”按钮，根据关键字过滤的威胁事件信息显示在事件列表中。

- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的威胁事件信息。点击右上角

下拉框，选择查看的平台，下方列表中将展示指定平台的威胁事件信息。当选择下级平台时，仅支持查看和导出威胁事件信息，不支持处置、标记状态等操作。

- 选择威胁事件的方向、源区域、目的区域或发生的时间范围，符合条件的威胁信息将展示在列表中。默认的时间范围为7天。

    - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
    - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- <综合视角>、<资产视角>、<攻击视角>标签页从不同视角展示了威胁事件详细信息。不同视角下，展示的威胁事件内容不同：
    - 点击“综合视角”，可查看事件的以下内容：“名称/时间”、“方向/威胁标签”、“检测引擎”、“级别”、“源IP/地理区域”、“目的IP/地理区域”、“状态”、“操作”。
    - 点击“资产视角”，可查看事件的以下内容：“名称/时间”、“级别”、“源IP/地理区域”、“源资产类型”、“目的IP/地理区域”、“目的资产类型”、“状态”、“操作”。
    - 点击“攻击视角”，可查看事件的以下内容：“名称/时间”、“方向/威胁标签”、“级别”、“IP地址”、“应用”、“协议”、“攻击阶段”、“状态”、“操作”。
- 点击列表上方 筛选 0 按钮，然后在弹出的部分选择筛选条件，系统将根据筛选条件筛选特定的威胁事件。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。

  说明：方向、时间以及筛选条件，可同时指定。
- 勾选列表上方“只看关注”复选框，列表中将展示被设为关注的威胁事件。
- 点击“聚合”处下拉菜单，选择列表所显示的内容的聚合方式，包括不聚合、按名称、按源IP以及按目的IP。
- 点击“导出”按钮，以CSV格式导出系统存储的前10000条威胁事件或者筛选、排序后的前10000条威胁事件信息。
- 事件的默认排序规则是按照“名称/时间”进行降序。点击表头中“名称/时间”或“级别”后的 按钮，可将事件进行重新排序：
    - 点击对应按钮后，当按钮显示为 时，将事件按照“名称/时间”或“级别”进行降序排列。

    - 点击对应按钮后，当按钮显示为 时，将事件按照“名称/时间”或“级别”进行降序排列。
    - 当“名称/时间”和“级别”后的按钮同时显示为 时，将事件进行随机排列。
- 点击列表中指定事件的“名称”链接，查看所选威胁的详细信息。
- 鼠标悬停于列表中指定事件的“状态”链接，在弹出菜单中选择“标记误报”或“标记已解决”，并选择标记的事件范围。标记范围包括当前威胁事件、该威胁的全部事件、指定源IP的威胁事件、指定目的IP的威胁事件或指定源IP&目的IP的威胁事件。
    - 标记为已解决后，指定威胁事件的状态列显示为“已解决”。标记为已解决的威胁事件，将不会参与到内网资产风险等级的评定中，但在下次检测时将会再次呈现报出。
- 标记为误报后，指定威胁事件的状态列显示为“误报”，且该威胁事件命中规则的误报数加1。标记为误报的威胁事件，将不会参与到内网资产风险等级的评定中，但是该威胁事件在下次检测时将会再次呈现报出。若标记的是挖矿类、DNS类、威胁情报类的部分威胁事件，标记后系统将继续弹出“是否将相关域名加入DNS类白名单？”的提示。选择“是”，该域名将被加入到“情报中心> 白名单 > DNS类白名单”中，该事件在下次检测时将不会再次呈报。选择“否”，则反之。
- 点击列表中指定威胁事件“操作”列的“加白名单”，在右侧弹出“加白名单”，页面中默认显示的是指定威胁事件的信息，包括源IP、目的IP和威胁名称，点击“确定”后，可以快速将该威胁事件加入全局白名单（情报中心>白名单>全局白名单），加入后将不再产生符合该条件的威胁事件。根据需要，用户可以点击源IP、目的IP或威胁名称的下拉框里修改为Any。 如需要查看、修改白名单条目，请参阅全局白名单。

  
  注意: 源IP、目的IP以及威胁名称不允许同时配置为Any。
- 点击列表中“操作”列的“处置”处下拉菜单，选择处置动作。针对所选威胁事件配置响应的处置动作，下发至指定的联动实体对威胁事件进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。

- 点击页面左下角 按钮，刷新事件列表。

查看威胁详细信息

在详细信息页面，可以查看所选威胁的描述信息、处置建议、详细分析结果、证据信息以及进程信息。



- **威胁信息**：根据匹配不同规则检测的威胁，<威胁信息>标签页内容也不同，如源信息、目的信息、命中的规则名称、服务器IP等。
  - 点击“规则名称”后的链接，在弹出的对话框中展示该规则的详细信息，包括命中次数、误报次数、级别以及描述信息。
  - 匹配“DNS域名是DGA”和“DGA域名恶意域名”的威胁事件会按照名称和源IP聚合，此时源信息和目的信息均与证据信息部分最新的一条信息保持一致。
- **证据信息**：展示威胁事件发生的数据源信息。 在<证据信息>标签页，展示指定威胁事件的数据源信息。
  - 在“操作”列，点击 图标，将证据信息报文从指定的存储位置中下载到用户本地。若该威胁事件不是本级平台的威胁事件，则不支持下载证据信息。
    注意：开启证据信息报文存储功能后，产生的威胁事件才可下载证据信息。详细操作，请参阅"证据信息管理" 在第495页。

    - 点击右上角 解码工具 图标，在<解码工具>页面输入需要解码的字符，解码后的内容展示在页面下方，方便用户对威胁事件进行分析。支持对URL编码和Base64编码进行离线解码。
    - 匹配“DNS域名是DGA”和“DGA域名恶意域名”的威胁事件会按照名称和源IP聚合，证据信息部分展示域名详情列表中各个域名对应的日志信息。
- **进程信息**：针对安装部署威胁溯源插件的用户主机，显示指定威胁事件相关联的进程信息详情，包括可执行程序、执行命令、执行时间等。
- **域名详情**：包含概述和列表两部分。仅有匹配“DNS域名是DGA”和“DGA域名恶意域名”的威胁事件包含该部分内容。在一段时间内，若发生上述两种威胁事件，则会按照名称和源IP聚合。
    - 一旦发现DGA域名就产生一条威胁事件提醒用户及时关注，概述部分形式如下供参考：“检测到主机195.190.133.65于2022-05-09 11:18:09发生了DGA事件，请及时关注”；在一段时间内相同源IP的DGA请求会进行聚合，一段时间过后，DGA事件聚合结束，此时会再次产生一条威胁事件，概述部分形式如下供参考：“检测到主机195.190.133.65于2022-05-09 11:18:09至2022-05-09 11:21:21之间共发生了60个DGA域名请求，只展示部分关键域名”。
      注意：关键域名即包含“IP地址”信息的域名，非关键域名的信息可在日志中查看。发生DGA域名请求的个数指访问域名的种类，即多次访问相同的域名时仅记录为一个域名请求。
    - 聚合列表展示DGA事件的域名、域名分类、域名标签、家族信息以及IP地址。最多展示20个域名，按照时间降序排列，同时优先展示包含“IP地址”信息的域名。
    - 鼠标悬停在“域名分类”、“域名标签”或“家族信息”列的信息上，查看该信息的详情。
- 点击页面右上角的“标记已解决”下拉列表，选择标记的事件范围，包括当前威胁事件、该威胁的全部事件、指定源IP的威胁事件、指定目的IP的威胁事件或指定源IP&目的IP的威胁事件。
    - 标记为已解决后，指定威胁事件的状态列显示为“已解决”。标记为已解决的威胁事件，将不会参与到内网资产风险等级的评定中，但在下次检测时将会再次呈现报出。
    - 点击 按钮，恢复状态为“未解决”。
- 点击页面右上角的“标记误报”下拉列表，选择标记的事件范围，包括当前威胁事件、该威胁的全部事件、指定源IP、指定目的IP或指定源IP&目的IP的威胁事件。若该威胁事件不是本级平台的威胁事件，则不支持标记状态。

- 标记为误报后，指定威胁事件的状态列显示为“误报”，且该威胁事件命中规则的误报数加1。标记为误报的威胁事件，将不会参与到内网资产风险等级的评定中，但是该威胁事件在下次检测时将会再次呈现报出。若标记的是挖矿类、DNS类、威胁情报类的部分威胁事件，标记后系统将继续弹出“是否将相关域名加入DNS类白名单？”的提示。选择“是”，该域名将被加入到“情报中心> 白名单 > DNS类白名单”中，该事件在下次检测时将不会再次呈报。选择“否”，则反之。
- 点击 按钮，恢复状态为“未解决”。

- **处置**：点击下拉菜单选择处置动作，针对所选威胁事件配置响应的处置动作，下发至指定的联动实体对威胁事件进行处理响应。处置动作包括：配置策略、IP阻断、访问控制、结束进程、隔离文件、重启终端、阻止非信任USB、USB白名单。若该威胁事件不是本级平台的威胁事件，则不支持配置处置动作。
- 点击页面右上角的 新建工单 按钮，在弹出对话框中新建工单，从而对威胁事件进行响应，并且通知到指定处理人实施人工处理。若该威胁事件不是本级平台的威胁事件，则不支持新建工单。

聚合威胁事件

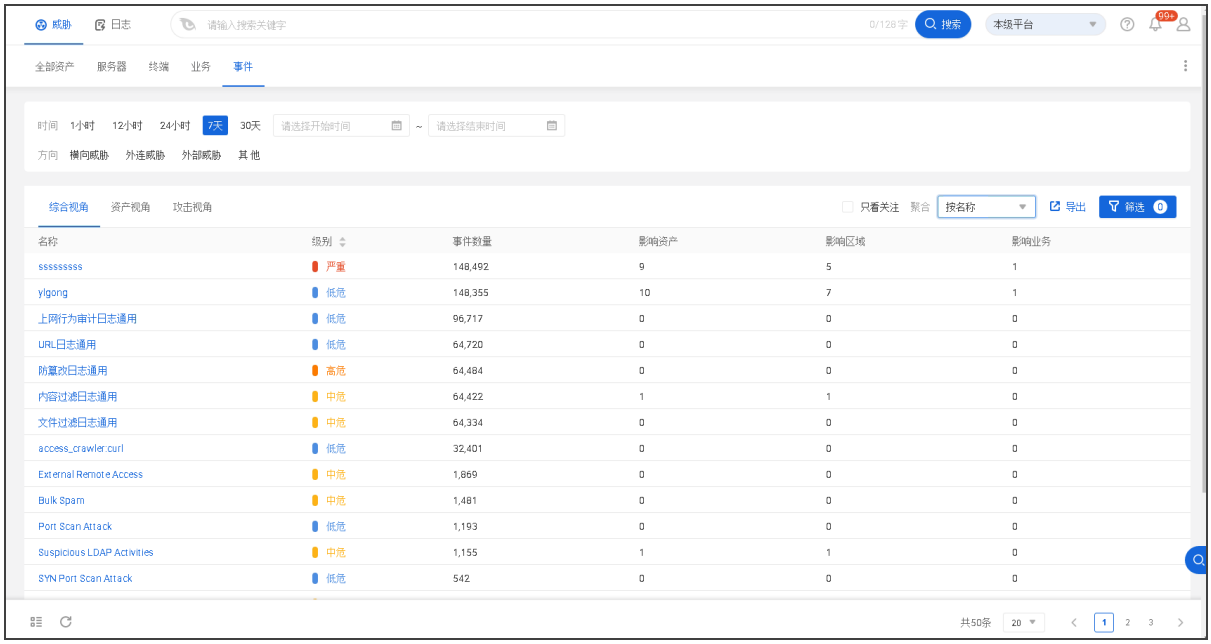
系统支持将名称、源IP或目的IP相同的威胁事件进行聚合展示，以图表的方式直观展示聚合威胁事件对全网（资产、区域、业务）的整体影响和趋势。

配置聚合威胁事件功能

配置聚合威胁事件功能，请按照以下步骤进行操作：

1. 点击“威胁分析”，打开威胁页面。
2. 点击<事件>标签页，打开事件列表页面。
3. 点击“聚合”处下拉菜单，选择列表所显示的内容的聚合方式，包括不聚合、按名称、按源IP以及按目的IP。

聚合后的威胁事件列表，如下图所示：



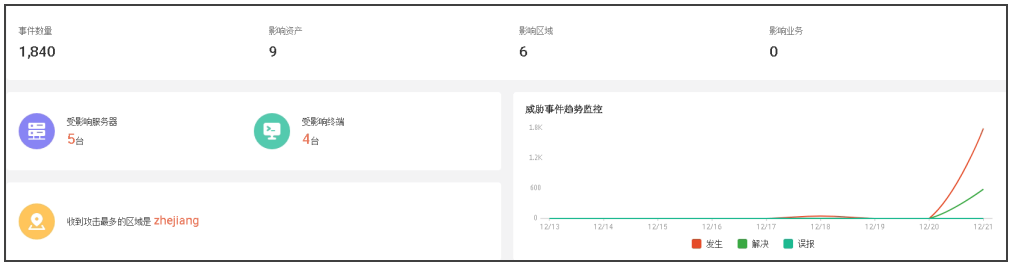
- 以列表方式展示出按照名称聚合的威胁事件名称、级别、被聚合的威胁事件数量、以及受该聚合事件影响的资产/区域/业务数。
- 点击聚合威胁事件名称，查看聚合威胁事件详细信息。

查看聚合威胁事件详细信息

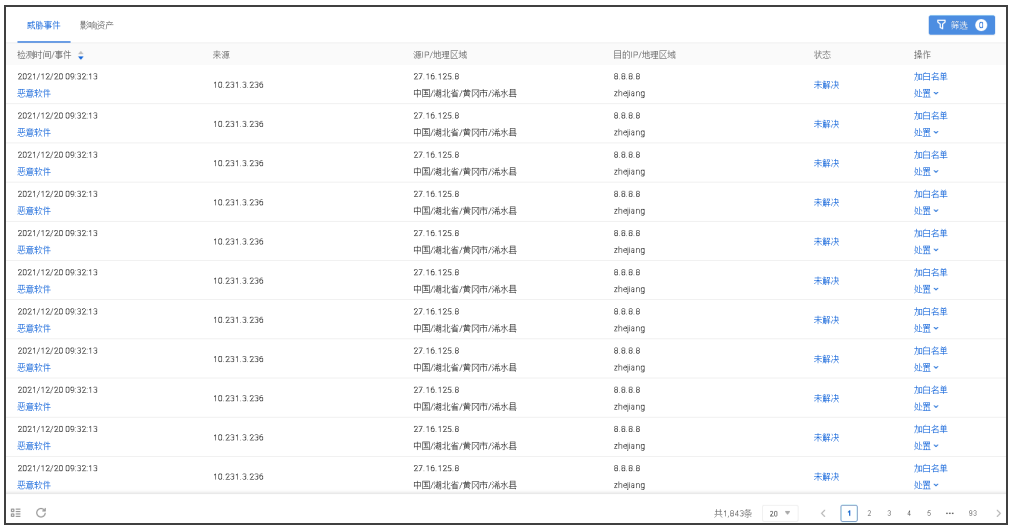
在聚合威胁事件详细信息页面，可以查看所选的聚合威胁事件的基本信息、事件的解决率、误报率、事件的影响范围、影响趋势以及详细的被聚合威胁事件列表。



- 该部分展示所选聚合威胁事件的基本信息，包括该威胁事件的处理率、所在的攻击阶段、类型、描述信息以及处置建议。
- 点击按钮，刷新聚合威胁事件详情页面。
- 页面右上角的时间与聚合威胁事件列表上方的时间保持一致。若需查看所选聚合威胁事件在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。



- 该部分展示所选聚合威胁事件的总数量、以及受该事件影响的资产、区域、业务的数量。
- 详细展示出受影响的服务器、终端对应的数量、以及受到攻击最多的区域名称。
- 右侧以曲线图的方式展示出所选威胁事件的趋势图。



- 该部分以列表方式展示被聚合的威胁事件、受影响的资产。
- 点击列表上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的威胁事件/影响资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 鼠标悬停于威胁事件列表中指定事件的“状态”链接，在弹出菜单中选择“标记误报”或“标记已解决”，并选择标记的事件范围。
- 点击威胁事件列表中的 按钮，在弹出对话框中新建工单，从而对威胁事件进行响应，并且通知到指定处理人实施人工处理。若该威胁事件不是本级平台的威胁事件，则不支持新建工单。

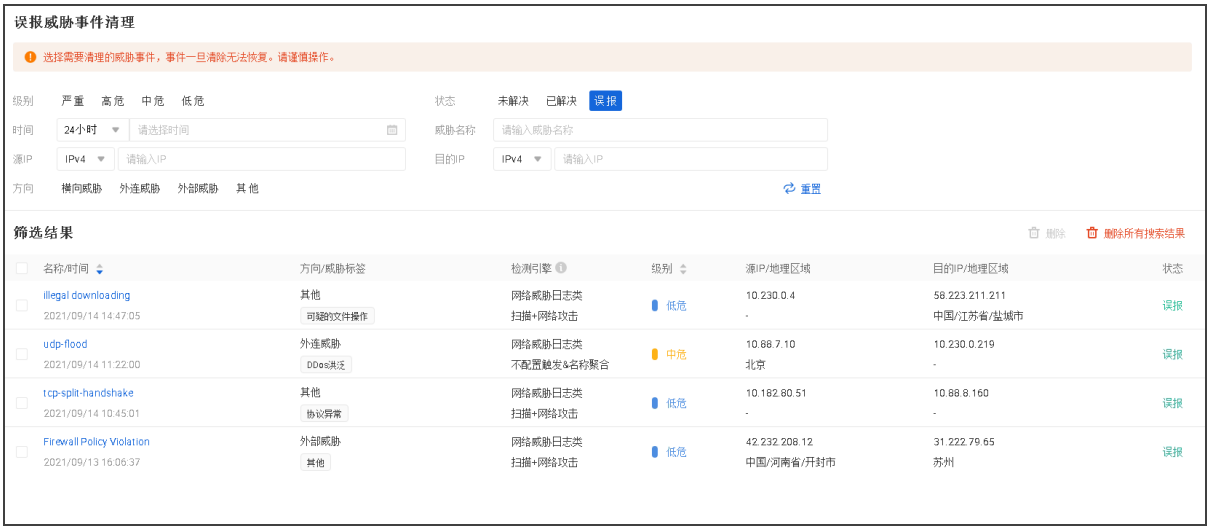
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新威胁事件/影响资产列表。

清理误报威胁事件

威胁事件被标记为“误报”后仍会在威胁事件列表中展示，当误报事件增加时可能会导致威胁分析页面加载缓慢，用户可以将需要清理的威胁事件从威胁事件列表中删除从而降低系统的误报率以及提高页面加载速度 。

清理误报威胁事件，请按照下列步骤操作：

1. 点击“威胁分析”，打开威胁页面，点击<事件>标签页，打开事件列表页面。
2. 当威胁事件被标记为“误报”后，鼠标悬停在状态列“误报”后的 上，将展示系统的提示文字，点击提示文字中的“点击此处进行管理”链接，跳转至<误报威胁事件清理>页面。



3. 在页面上方可以根据需要指定筛选条件，过滤出需要删除的威胁事件，展示在下方的“筛选结果”列表中。点击 重置 ，可以将筛选条件重置为默认状态。

威胁事件筛选条件配置说明

选项	说明
级别	指定威胁事件的威胁等级，包括严重、高危、中危以及低危。点击指定的威胁等级按钮添加筛选条件，再次点击将清除筛选条件。

选项	说明
状态	指定威胁事件的状态，包括未解决、已解决以及误报。点击指定的状态按钮添加筛选条件，再次点击将清除筛选条件。默认情况下，仅选中误报状态。
时间	指定威胁事件发生的时间。在下拉框中选择1小时、12小时、24小时、7天、30天以及自定义。当选择“自定义”时，可以在右侧的弹出框中指定开始时间和结束时间，若不指定开始时间和结束时间，则筛选结果中会展示所有时间段的威胁事件。默认情况下，时间指定为24小时。
威胁名称	指定威胁事件的名称。在文本框中输入威胁名称，系统支持对威胁名称进行模糊搜索。
源IP	指定威胁事件的源IP。在下拉框中选择IP地址的类型为IPv4或IPv6，在右侧的文本框中输入源IP地址。系统支持对源IP进行模糊搜索。
目的IP	指定威胁事件的目的IP。在下拉框中选择IP地址的类型为IPv4或IPv6，在右侧的文本框中输入目的IP地址。系统支持对目的IP进行模糊搜索。
方向	指定威胁事件的方向，包括横向威胁、外连威胁、外部威胁和其他。点击指定的方向按钮添加筛选条件，再次点击将清除筛选条件。

4. 在页面下方的“筛选结果”列表中，勾选指定威胁事件前的复选框，点击右上角的“删除”可以批量删除指定威胁事件；若要删除当前页面展示的筛选到的全部威胁事件，勾选“名称/时间”前复选框，点击右上角的“删除”进行操作；若要删除筛选到的所有威胁事件，直接点击右上角“删除所有搜索结果”。



注意: 威胁事件一旦被清除将无法恢复，请谨慎操作。

日志

以表格等方式展示指定时间段的日志信息，方便用户对威胁数据源进行查看和检索。日志信息来自于山石网科安全设备、流量探针和用户主机，包括Syslog、NetFlow、Meta Data、Sysmon以及Linux五种类型。

- **Syslog**：所有来自山石网科安全设备的Syslog类型的日志信息，例如威胁日志、事件日志、会话日志、NAT日志、网页安全日志、防篡改日志等。
- **NetFlow**：所有来自山石网科安全设备或流量探针的NetFlow类型的日志信息，是与NetFlow功能相关的日志信息，统计记录网络中数据包的源\目的地址、端口号等信息。
- **Meta Data**：所有来自流量探针的日志信息，是指网络设备的镜像流量经过流量探针解析、分析、提取后的元数据信息。
- **Sysmon**：所有来自装有威胁溯源插件的用户主机的日志信息，包含威胁溯源插件采集到的主机进程创建、网络访问、文件操作、注册表修改等相关行为信息。
- **Linux**：所有来自Linux系统的设备并且符合Syslog协议的Linux日志信息。

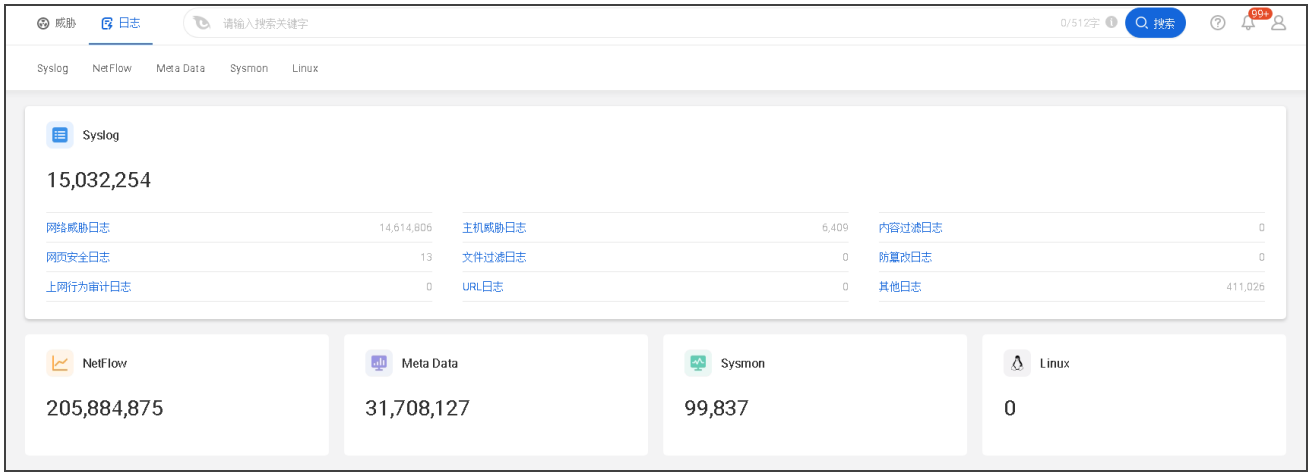


注意:

- 只有当用户在“日志源管理”页面配置了日志源并且开启接收日志源的Syslog类型日志、NetFlow类型日志后，才可在“日志”页面查看到采集的所有来自山石网科安全设备的Syslog类型、NetFlow类型的日志。关于日志源的配置，请参阅“日志源管理”。
- 只有当用户在“探针管理”页面开启接收流量探针的数据源信息，才可在“日志”页面查看到采集的所有来自流量探针的Meta Data类型的日志。关于探针的配置，请参阅“"探针管理" 在第497页”。
- 只有当用户在流量探针的“系统状态”页面，开启发送“NetFlow日志”到智源平台功能，才可以在“日志”页面查看到采集的所有来自流量探针的NetFlow类型的日志。关于流量探针的配置，参见“智源流量探针WebUI用户手册”。

日志概览

日志概览页面为用户展示指定时间周期内的Syslog、NetFlow、Meta Data、Sysmon以及Linux五种类型日志的数量等信息。点击“威胁分析”，进入威胁分析页面。在威胁分析页面，点击 日志 按钮，进入日志概览页面。

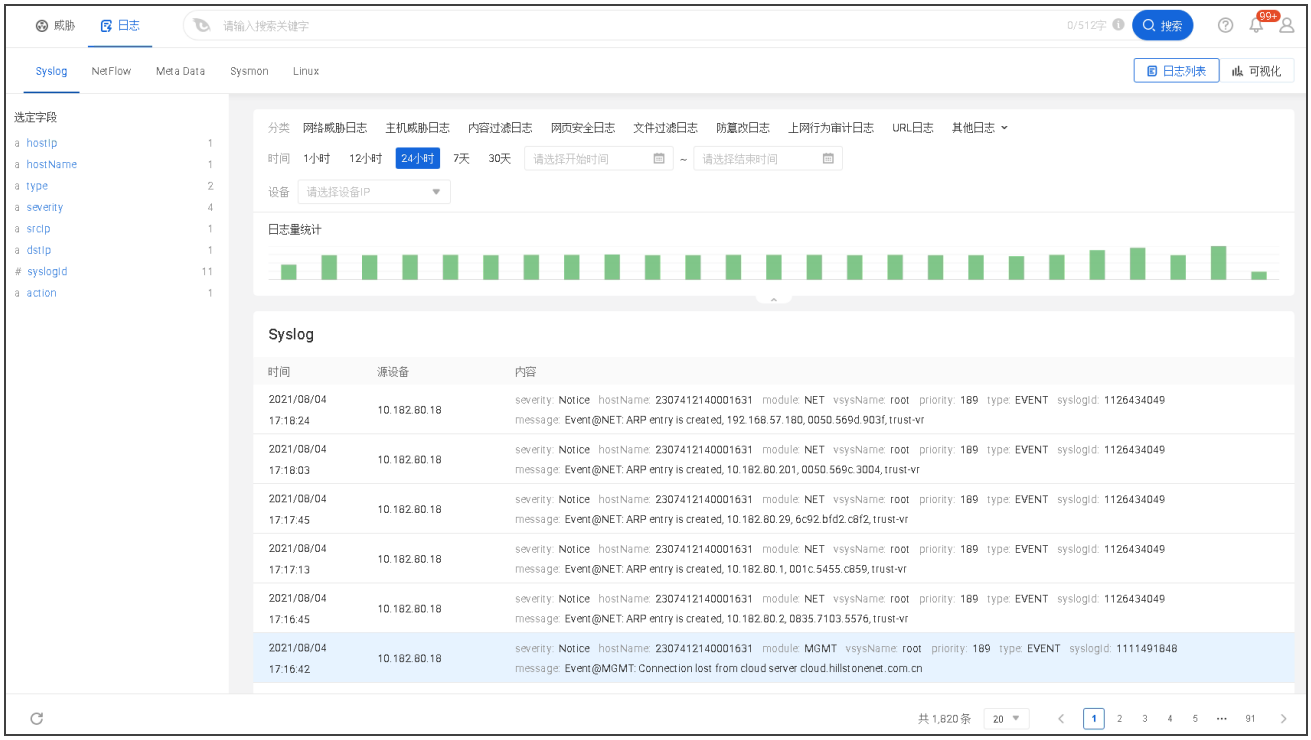


- Syslog：展示采集的所有来自山石网科安全设备的Syslog类型的日志的总数量以及子类型日志数量。
  - 点击总数量链接，打开Syslog列表页面，最近24小时内的日志显示在Syslog列表中（超过10000条时，系统仅显示10000条）。
  - 点击总数量下方的子类型名称链接，打开Syslog列表页面，所选类型的日志显示在Syslog列表中。
- NetFlow：展示采集的所有来自山石网科安全设备或流量探针的NetFlow类型的日志的数量。
  - 若要采集所有来自山石网科安全设备的NetFlow类型的日志，在山石网科安全设备的NetFlow Profile页面，配置服务器IP地址为智源平台的IP地址。关于NetFlow的具体信息，参见“StoneOS WebUI用户手册”。
  - 若要采集来自流量探针的NetFlow类型的日志，在流量探针的“系统状态”页面，开启发送“NetFlow日志”功能。关于流量探针的配置，参见“智源流量探针WebUI用户手册”。
  - 点击数量链接，打开NetFlow列表页面，最近24小时内的日志显示在NetFlow列表中（超过10000条时，系统仅显示10000条）。

- Meta Data：展示采集的所有来自流量探针的日志的数量。
    - 点击数量链接，打开Meta Data列表页面，最近24小时内的日志显示在Meta Data列表中（超过10000条时，系统仅显示10000条）。
- Sysmon：展示采集的所有来自装有威胁溯源插件的用户主机的日志的数量。
    - 点击数量链接，打开Sysmon列表页面，最近24小时内的日志显示在Sysmon列表中（超过10000条时，系统仅显示10000条）。
- Linux：展示采集的所有来自Linux系统的设备并且符合Syslog协议的Linux日志的数量。
    - 点击数量链接，打开Linux列表页面，最近24小时内的日志显示在Linux列表中（超过10000条时，系统仅显示10000条）。

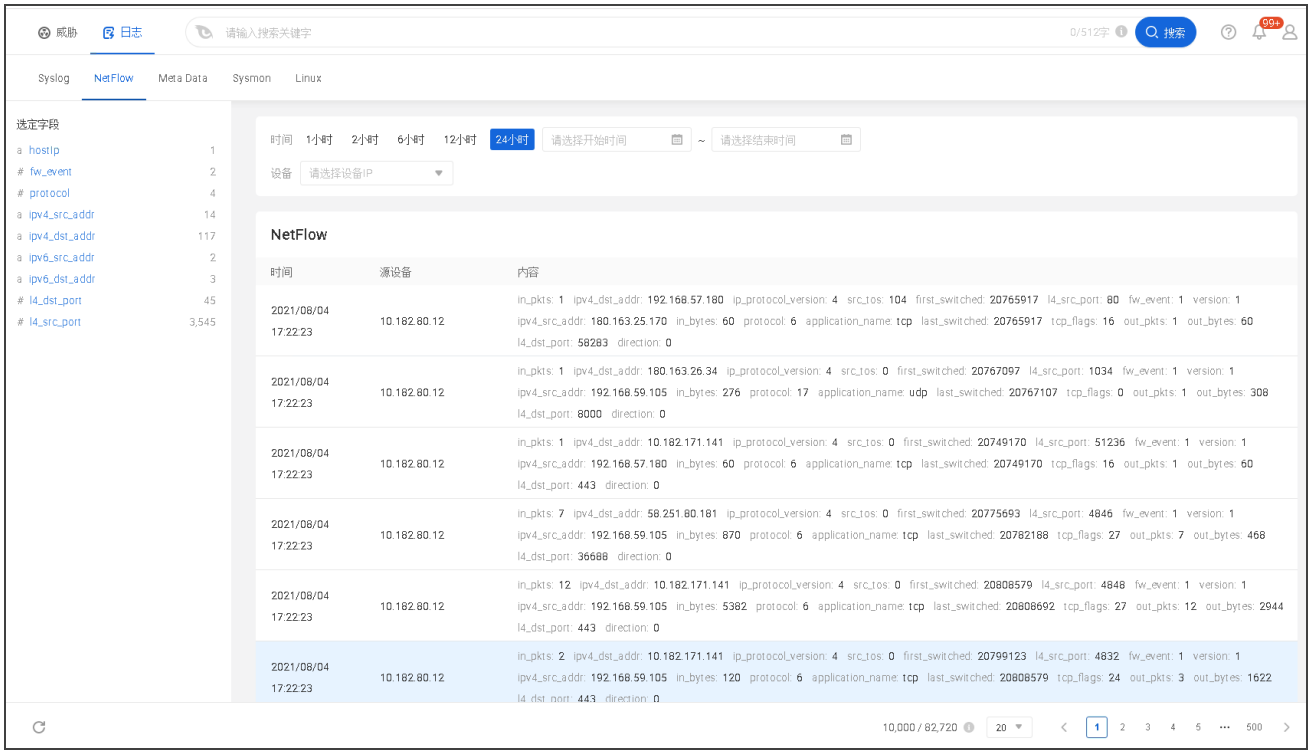
Syslog列表

Syslog列表页面统计并展示指定类型或时间段内，所有来自山石网科安全设备的Syslog类型的日志信息。点击“威胁分析”，进入威胁分析页面。在威胁分析页面，点击 日志 按钮，点击<Syslog>标签页，打开Syslog列表页面。用户可在此页面进行日志搜索和查看。



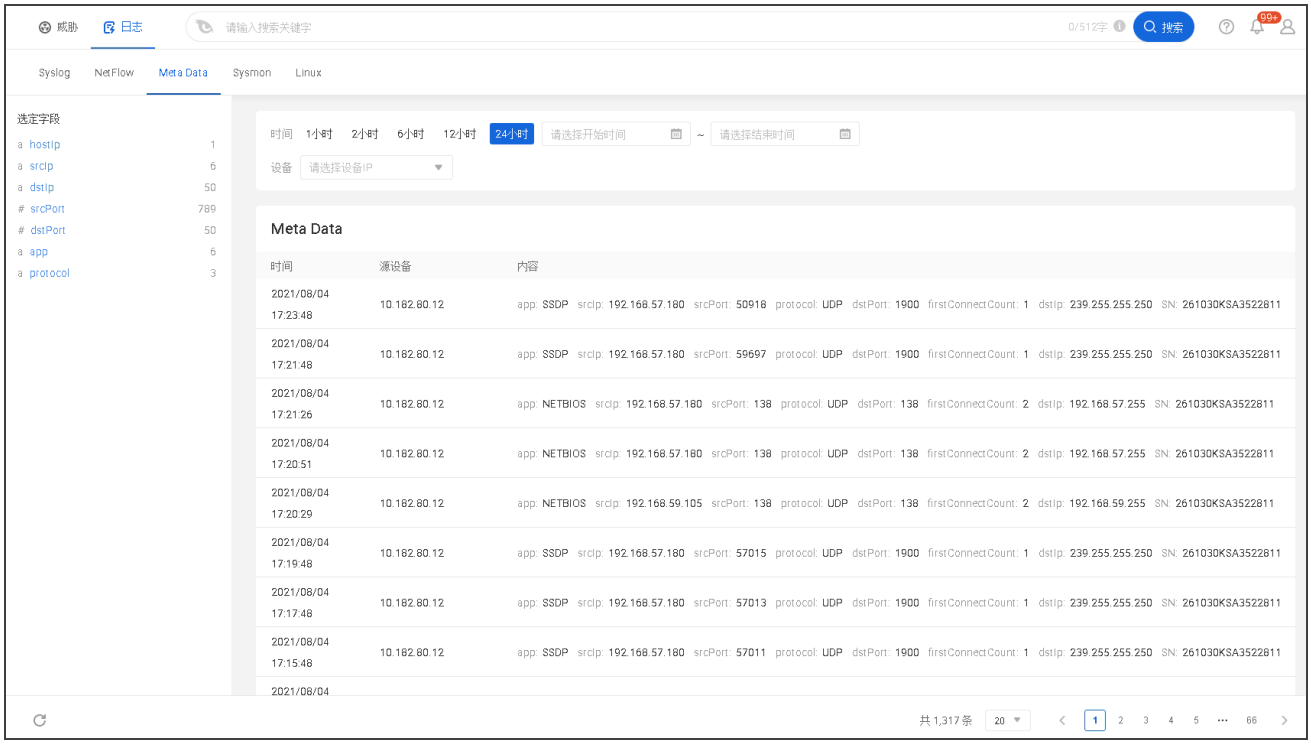
NetFlow列表

NetFlow列表页面统计并展示指定时间段内，所有来自山石网科安全设备或流量探针的NetFlow类型的日志信息。点击“威胁分析”，进入威胁分析页面。在威胁分析页面，点击 日志 按钮，点击<NetFlow>标签页，打开NetFlow列表页面。用户可在此页面进行日志搜索和查看。



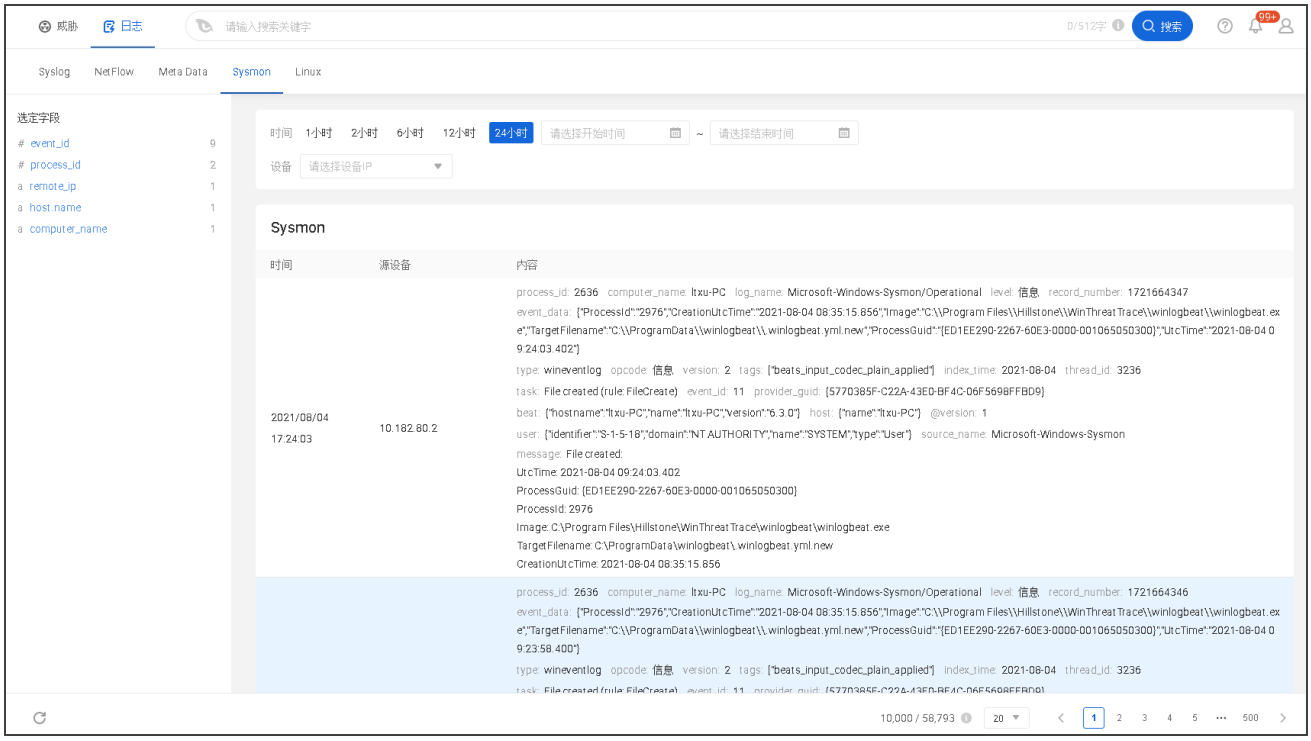
Meta Data列表

Meta Data列表页面统计并展示指定时间段内，所有来自流量探针的Meta Data类型的日志信息。点击“威胁分析”，进入威胁分析页面。在威胁分析页面，点击 日志 按钮，点击<Meta Data>标签页，打开Meta Data列表页面。用户可在此页面进行日志搜索和查看。



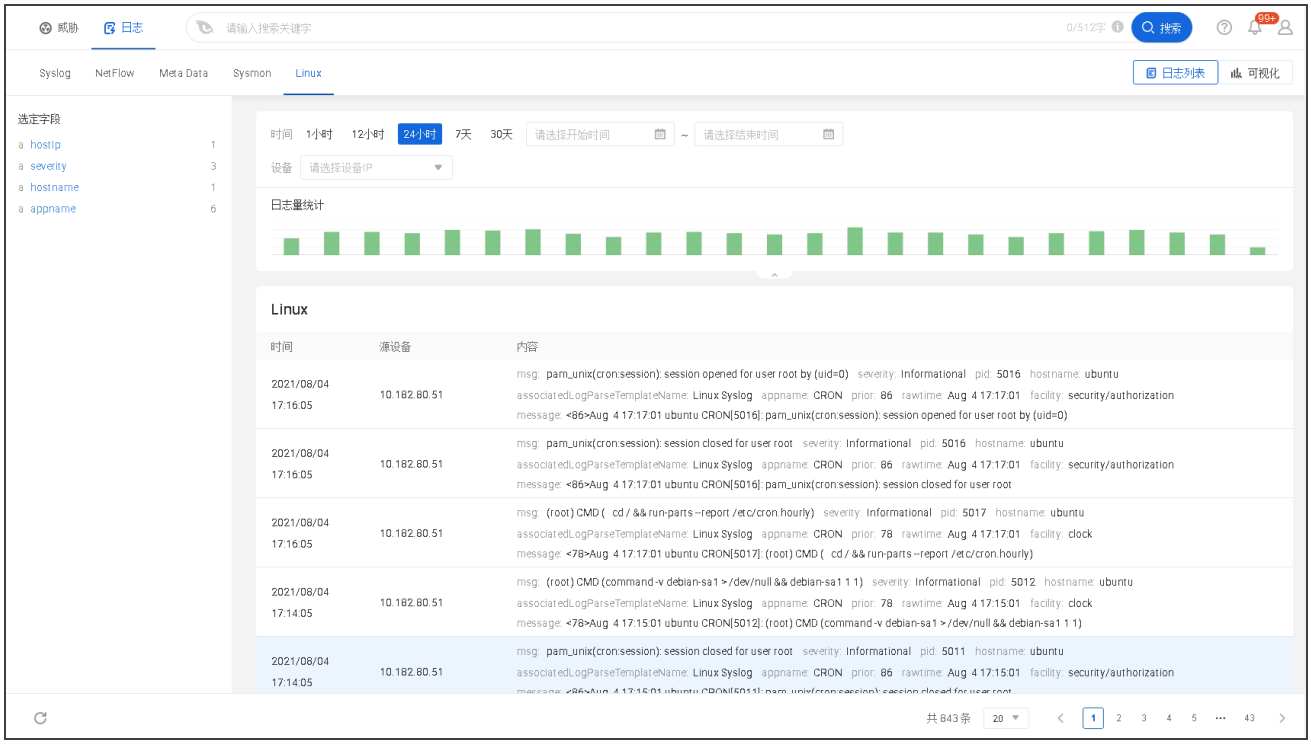
Sysmon列表

Sysmon列表页面统计并展示指定时间段内，所有来自安装威胁溯源插件的用户主机的Sysmon类型的日志信息。点击“威胁分析”，进入威胁分析页面。在威胁分析页面，点击 日志 按钮，点击<Sysmon>标签页，打开Sysmon列表页面。用户可在此页面进行日志搜索和查看。



Linux列表

Linux列表页面统计并展示指定时间段内，所有来自Linux系统的设备并且符合Syslog协议的Linux日志信息。点击“威胁分析”，进入威胁分析页面。在威胁分析页面，点击 日志 按钮，点击<Linux>标签页，打开Linux列表页面。用户可在此页面进行日志搜索和查看。



日志搜索

对于Syslog、NetFlow、Meta Data、Sysmon以及Linux五种类型日志的搜索方法基本相同，具体请参考以下步骤：

1. 点击“威胁分析”，进入威胁分析页面。

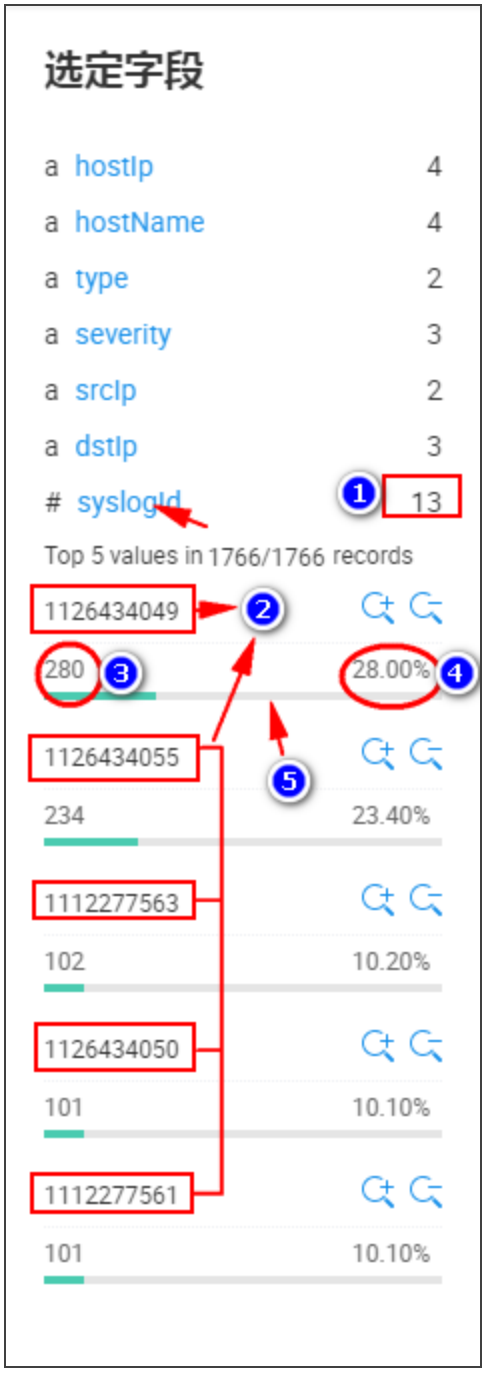
2. 在威胁分析页面，点击 日志 按钮，点击<Syslog/NetFlow/Meta Data/Sysmon/Linux>标签页，打开对应的日志页面。

3. 点击页面上方的“请输入搜索关键字”文本框，自动展开历史记录。点击历史记录或直接输入关键字后，点击“搜索”按钮，根据关键字过滤的相应类型的日志信息显示在下方列表中，列表上方将显示“系统当前显示的日志总数/数据库中搜索到的日志总数”(如10000/456711表示当前列表中显示了10000条搜索结果，而实际数据库中有456711条搜索结果)。

4. 鼠标悬停或点击搜索框中处，弹出搜索帮助说明，用户需要按照规定的格式进行搜索。搜索格式说明如下：

- 格式为 "字段:值"，如 srcIp:10.180.173.56。"值"支持普通文本或正则表达式（如/^sdh/）。
- 如果"值"为普通文本，且包含以下字符：+-=&&||><!(){}[]^"~*?:\/，需要在字符前添加转义符反斜杠"\"，或者为文本添加双引号。如 outInterface:ethernet0\/5或者out-Interface:"ethernet0/5"。
- 支持使用 "AND" 或者 "OR" 连接多个搜索条件。如 srcIp:10.180.173.56 AND srcPort:38718 AND outInterface:"ethernet0/5"。
- 支持使用圆括号实现条件嵌套。如 (srcIp:10.180.173.56 AND srcPort:38718 AND out-Interface:"ethernet0/5") OR (srcIp:"1.1.1.1" AND (dstIp:2.2.2.2 OR AND type:Session)。
- 使用"-"号做排除。如排除威胁事件 (-type:THREAT)。

5. 若需搜索某种类型的日志，可点击“分类”后的对应日志类型进行搜索，符合条件的日志信息将展示在列表中（当前仅Syslog日志支持分类）。如需选择“其他日志”分类的日志，点击“其他日志”在展开分类中勾选需要的日志类型复选框或勾选“全选”复选框进行选择，已选择的其他日志类型数量将显示在“其他日志”处。
6. 若需搜索某个时间范围的日志，可直接点击“1小时/2小时/24小时/3天/7天/30天”或选择具体的开始时间和结束时间进行搜索，符合条件的日志信息将展示在列表中。
7. 在“设备”下拉菜单中选择设备IP地址，按照指定设备IP进行搜索，符合条件的日志信息将展示在列表中。
8. 对于Syslog类型日志信息、Linux日志信息，在“日志量统计”部分，使用柱状图形式展示指定分类、指定设备或者指定时间范围内的日志数量趋势统计结果。
9. 点击页面左下角 按钮，可刷新日志列表，实时刷新出最新的日志信息。
10. 另外，系统根据日志内容中的Json字符串（格式为 "字段:值"）进行了分类和聚合，供用户进行快速搜索和查看。日志列表左侧的“选定字段”是系统选出的一些通用的日志Json字符串“字段”。点击任一“选定字段”，在该字段下方将显示日志数量排名前5的"值"，并显示该“值”对应的日志数量和占比。**注意**：此处的排名、日志数量及占比均是基于右侧日志列表中显示的日志总数来计算的。
    如下图，点击选定字段“syslogid”,将展开如下信息：



- 标识“1”表示当前显示的日志中syslogid字段的不同“值”共有13种；
- 标识“2”为日志个数排名前5的“值”（如：1126434049为syslogid字段的其中一个值）；
- 标识“3”表示syslogid=1126434049的当前日志个数为280个；

- 标识“4”表示syslogid=1126434049的日志数量占当前日志总数的百分比；
- 标识“5”表示syslogid=1126434049的日志的所占比例的条形图；
- 图中“Top 5 Values in 1766/1766 records.”中的“1766/1766”表示“含有syslogid字段的日志数量/右侧日志列表中显示的日志总数”。
- 点击  按钮，该“值”将作为搜索项被添加到搜索框，然后日志列表将显示搜索结果；
- 点击  按钮，该“值”将作为排除条件被添加到搜索框中，然后日志列表将显示排除后的结果。

11. 点击日志列表中“内容”列中的Json字符串中的"字段"或"值"（如“severity： Notice”，其中severity为"字段"，Notice为"值"），将弹出搜索下拉菜单，供用户进行选择搜索；同时下拉单选项中还显示了搜索后的日志数量（“新搜索”暂不显示）。**注意**：此处显示的日志数量均是基于数据库中所有日志搜索出的结果。
    - 添加到搜索：系统会将选中的“字段"和"值"添加到当前的搜索框中，然后日志列表将显示搜索后的结果。
    - 从搜索中排除：系统会将选中的“字段"和"值"作为排除条件添加到当前搜索框中，然后日志列表将显示排除后的结果。
    - 新搜索：系统将清空原先的搜索条件，选中的“字段"和"值"作为一个新的搜索条件添加到搜索框中，然后日志列表将显示搜索后的结果。



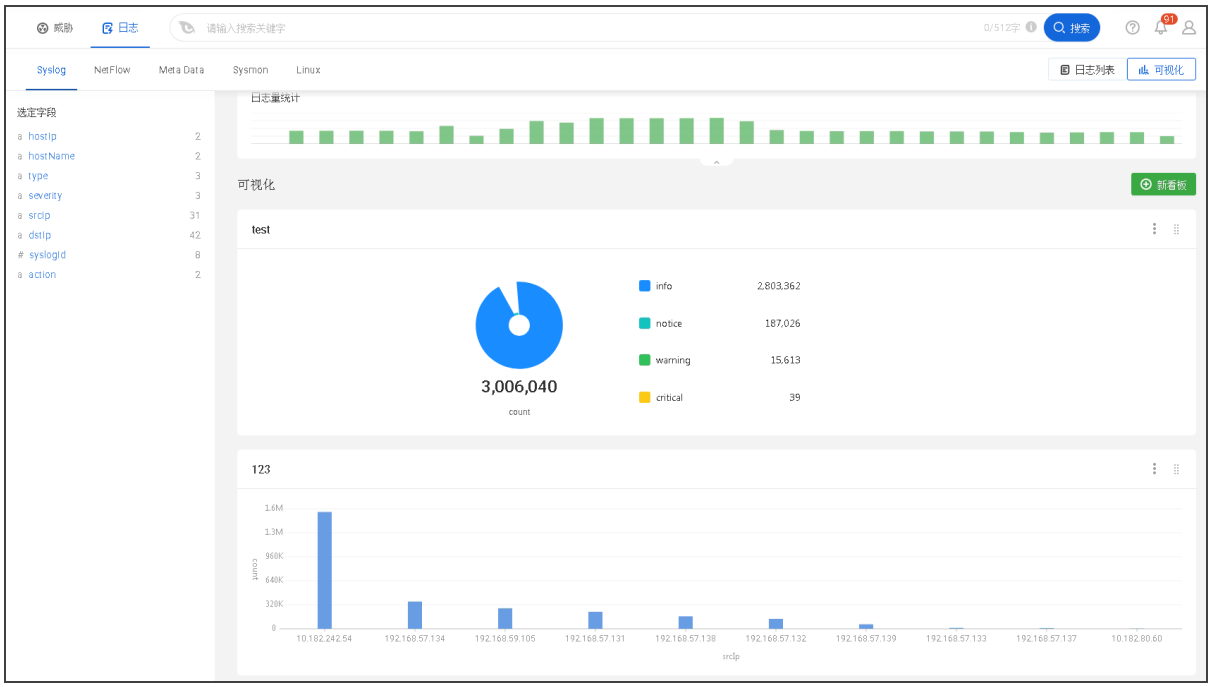
注意:

- 关键字搜索、日志分类、时间和筛选条件可同时指定，用户可根据需要进行自由组合搜索。
- 字段“message”不支持上述步骤9中的点击后搜索功能。

可视化展示

对于Syslog类型的日志信息、Linux日志信息搜索结果，用户可创建看板，指定不同的聚合统计方式使用柱状图、折线图、玫瑰图、圆环图形式可视化展示聚合搜索结果。

在威胁分析页面，点击 日志 按钮，在<Syslog>标签页中，点击右上角 可视化 按钮，打开可视化页面。



- 点击“可视化”部分的“+”或点击“新看板”按钮，创建日志可视化看板。当前系统最多可创建10个看板。
- 修改/删除看板：在看板页面的右上角，点击“ ⋮ ”编辑或删除看板内容。
- 移动看板：在看板页面的右上角，长按“ ⠿ ”并拖拽看板，可移动其位置，与其他看板更换位置。

创建日志可视化看板

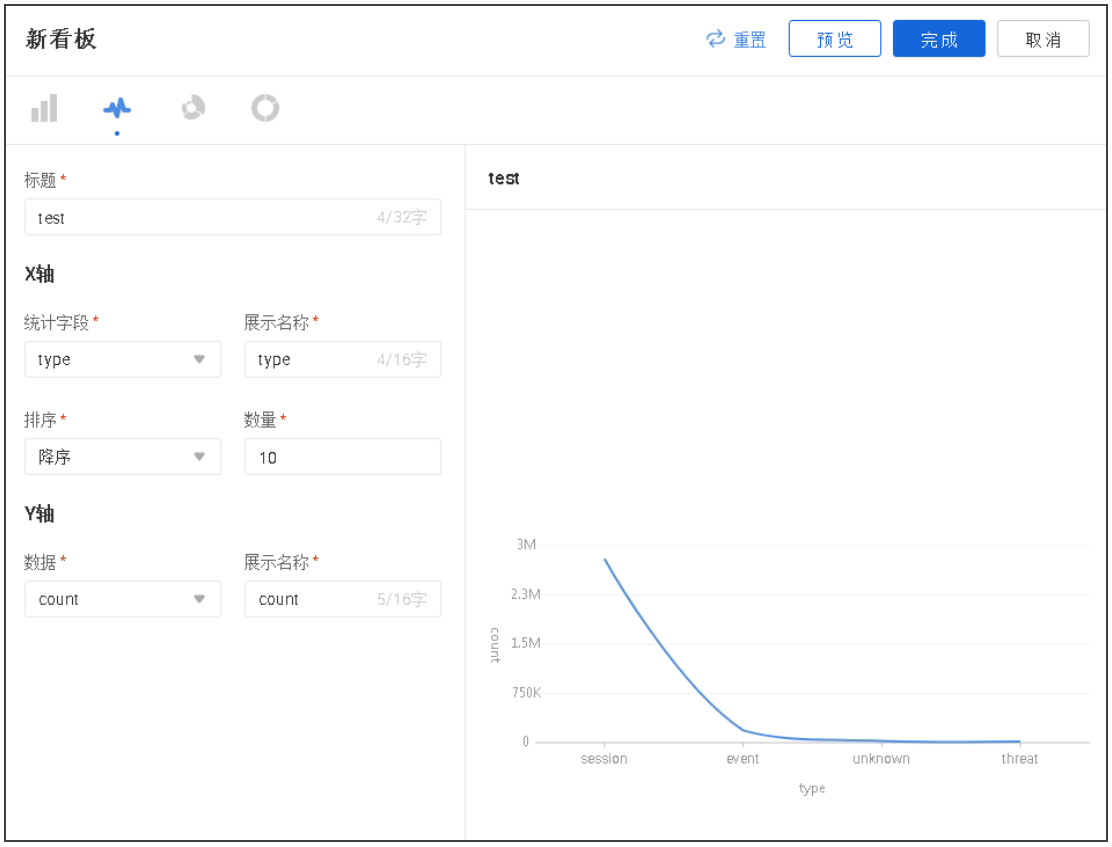
创建日志可视化看板，请按照以下步骤进行操作：

1. 点击“威胁分析”，进入威胁分析页面。

2. 在威胁分析页面，点击 日志 按钮。

3. 选择<Syslog/Linux>标签页，点击右上角 可视化 按钮，打开可视化页面。

4. 点击“可视化”部分的“+”或点击“新看板”按钮，创建日志可视化看板。



填写看板配置的相关参数。

选项	说明
图表类型	选择图标，指定图标的图示类型。 表示柱形图，表示折线图，表示玫瑰图，表示圆环图。

选项	说明
标题	指定看板的标题。
X轴（柱形图/折线图）	
统计字段	点击下拉菜单选择聚合统计的字段名称，例如，选择“srcip”，柱形图/折线图的X轴将按照源IP聚合统计日志搜索结果。 **注意**：不同日志信息对应可选择的统计字段不同。仅日志列表左侧系统默认的“选定字段”支持作为统计字段用于聚合统计。
展示名称	指定X轴数据的展示名称，根据“统计字段”的选择，“展示名称”文本框显示默认名称，用户可以修改为其他自定义名称。范围是1到16个字。
排序	选择图标的排序方式，升序或降序。默认为降序。
数量	指定X轴中显示的统计个数。默认数量为10，范围是1到15。
Y轴（柱形图/折线图）	
数据	指定Y轴的数据类型，目前仅支持数量“count”。
展示名称	指定Y轴数据的展示名称。范围是1到16个字。目前默认为数量“count”。
类别（玫瑰图/圆环图）	
统计字段	点击下拉菜单选择聚合统计的字段名称，例如，选择“srcip”，玫瑰图/圆环图的X轴将按照源IP聚合统计日志搜索结果。 **注意**：不同日志信息对应可选择的统计字段不同。仅日志列表左侧系统默认的“选定字段”支持作为统计字段用于聚合统计。
排序	选择图标的排序方式，升序或降序。默认为降序。
数量	指定玫瑰图/圆环图中显示的统计个数。默认数量为10，范围是1到15。

选项	说明
计数（玫瑰图/圆环图）	
数据	指定玫瑰图/圆环图的数据类型，目前仅支持数量“count”。
展示名称	指定玫瑰图/圆环图数据的展示名称。范围是1到16个字。目前默认为数量“count”。

5. 点击右上角“预览”按钮，<新看板>页面右侧将显示预览图。

6. 如需清空配置项，点击“重置”按钮。

7. 点击“完成”，保存配置，返回至可视化页面，新创建的看板显示在该页面中。

第4章 弱点分析

弱点扫描是指基于弱点数据库，使用一些软件或硬件工具通过扫描等手段对指定的计算机系统的安全脆弱性进行检测，发现可利用漏洞、弱点的一种安全检测行为。

系统提供弱点分析功能，用户可以在智源平台中添加被管理的扫描器设备、配置弱点扫描任务并下发至扫描器、配置弱点报告获取任务用于从扫描器获取弱点报告、手动导入弱点报告，在智源平台进行统一管理并分析扫描器的弱点扫描结果，以列表的方式展示弱点详细信息、发现弱点的主机，从而帮助用户对风险资产的安全脆弱性进行全面了解。



注意:

- 目前，系统仅支持对Nessus的.nessus格式扫描报告、绿盟RSAS的xml格式报告、山石网科RAS（远程安全评估系统Remote Assessment System）的测评能手xml格式报告进行分析。（测评能手xml格式为测评中心的通用xml模板）
- 弱点扫描任务仅支持下发至山石网科RAS设备。
- 在使用“弱点分析”功能之前，为保证弱点信息展示效果更佳，建议用户先升级到最新版本的“山石弱点情报库”。关于升级方法，请参阅"威胁情报库" 在第320页。
- 对于导入的相同主机的弱点扫描报告（手动导入或根据报告获取任务、扫描任务自动获取），系统仅解析该主机的最新弱点报告。

弱点分析部分包含如下内容：

- "弱点分析" 在第162页：介绍如何手动导入扫描报告结果、以及根据获取的报告查看发现弱点的主机列表以及所有弱点详细列表。
- "弱点报告获取" 在第167页：介绍如何配置弱点报告获取任务，根据指定的任务周期从扫描器上自动获取扫描报告。
- "弱点扫描任务" 在第169页：介绍如何配置下发到任务指定的被管理的扫描器设备中的扫描任务。

- "扫描器配置" 在第173页：介绍如何查看、添加扫描器。
- "弱点分析配置案例" 在第176页：介绍完整的弱点分析配置案例。

弱点分析

弱点分析页面以列表的方式展示了发现弱点的主机（匹配资产管理中的已有内网资产）、以及弱点报告中的所有弱点信息。

导入弱点报告

导入本地弱点报告，请按照以下步骤进行操作：

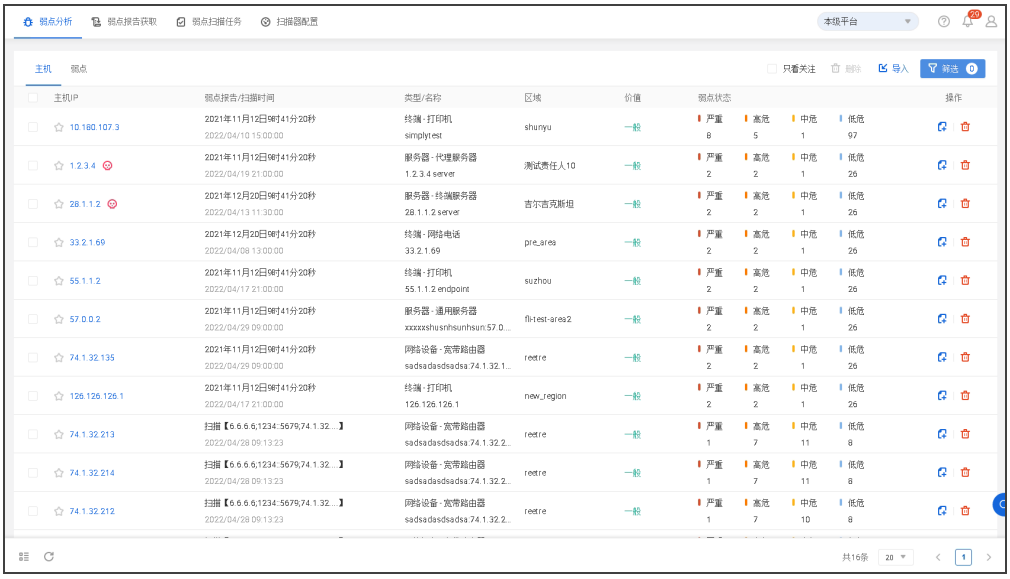
1. 点击“弱点分析>弱点分析”。
2. 点击页面右上角 

按钮，打开“导入报告”页面。
3. 点击“厂商”下拉菜单，选择生成弱点报告的厂商，目前包括NESSUS、绿盟RSAS、山石网科RAS。
4. 点击“选择文件”按钮，选择本地的NESSUS弱点报告文件、绿盟RSAS的xml格式报告文件或者山石网科RAS的测评能手xml格式报告文件。
5. 点击“上传”按钮，上传已选择的弱点报告文件。

主机

当扫描器扫描出发现弱点的主机（服务器或终端），并且该主机是已经在“资产管理”中添加的内网资产，那么将会在主机列表中显示该主机信息，包括主机IP地址、所属弱点报告的名称、扫描时间、主机对应的资产类型、资产名称、资产所属区域、价值以及该主机发生的各级别弱点个数，当查看下级平台的数据时，列表中还会展示该平台的名称和IP地址。

点击“弱点分析>弱点分析>主机”，打开主机列表页面。



- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的主机信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的主机信息。当选择下级平台时，仅支持查看主机信息，不支持新建工单、导入弱点报告、删除资产或关注资产操作。

- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的主机。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。

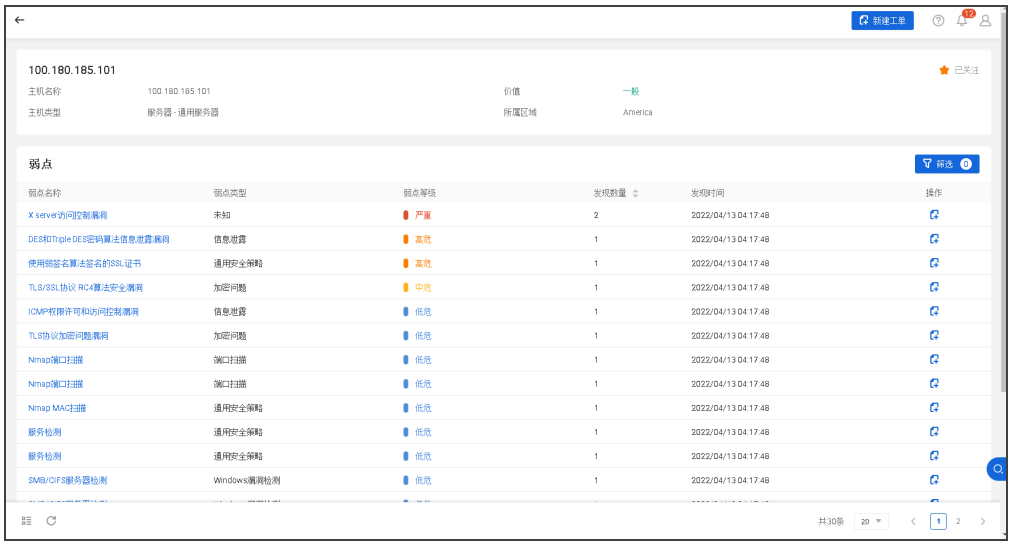
- 点击列表中具体资产前的 ☆ 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。

- 勾选列表上方“只看关注”前的复选框，列表中将展示所有被设为重点关注的资产。

- 点击主机列表中主机条目后的 按钮，或者在主机详情页面点击“新建工单”按钮，配置对应的工单对发现弱点的主机进行响应。若该主机不是本级平台的主机，则不支持新建工单。

- 点击主机列表中主机条目后的 按钮，删除所选主机。如需批量删除主机，勾选多个主机条目，点击右上角“删除”按钮。

- 点击“主机IP”链接，打开所选主机的详情页面，查看该主机对应的资产信息、发现的所有弱点列表。



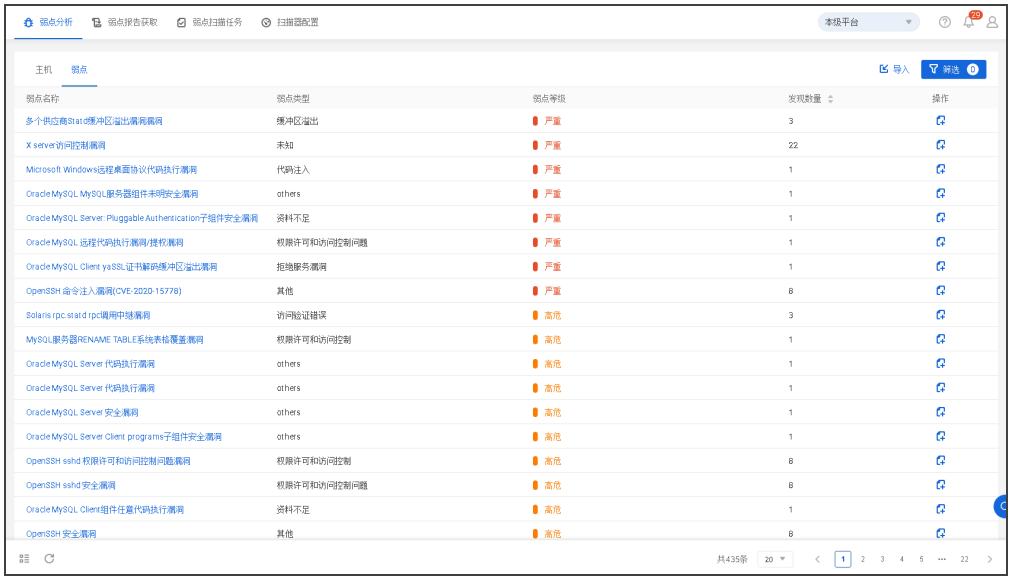
- 点击 

按钮，导入弱点报告，详细步骤请参阅导入弱点报告。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新主机列表。

弱点

弱点列表展示根据扫描器的弱点报告（手动导入、报告获取任务获取或者扫描任务获取）分析出的所有弱点信息，包括弱点名称、类型、等级、数量等，当查看下级平台的数据时，列表中还会展示该平台的名称和IP地址。

点击“弱点分析>弱点分析>弱点”，打开弱点列表页面。

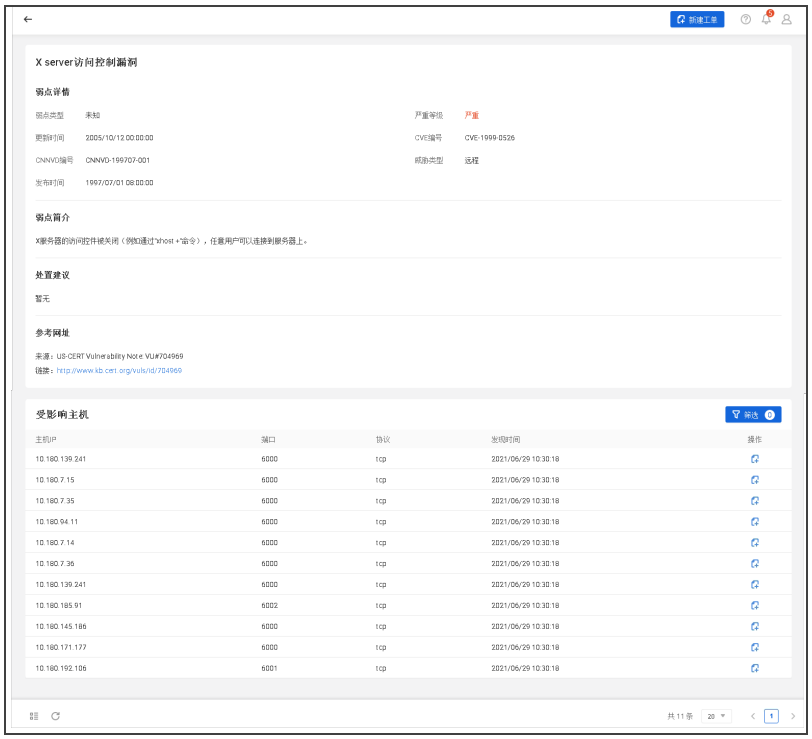


- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的弱点信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的弱点信息。当选择下级平台时，仅支持查看弱点信息，不支持新建工单和导入操作。

- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。

- 点击弱点列表中弱点条目后的按钮，或者在弱点详情页面点击“新建工单”按钮，配置对应的工单对弱点进行响应。若该弱点不是本级平台的弱点，则不支持新建工单。

- 点击弱点名称链接，打开所选弱点的详情页面，查看该弱点详细信息、简介、处置建议、参考网站以及受影响的主机列表。



- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新弱点列表。

弱点报告获取

用户可以配置弱点报告获取任务，根据指定的任务周期从扫描器上自动获取扫描报告，并且自动将弱点扫描结果呈现在智源平台中。用户可以在“弱点分析”页面查看相关弱点信息。

查看弱点报告获取任务

点击“弱点分析>弱点报告获取”，打开弱点报告获取任务列表页面，查看所有弱点报告获取任务。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点报告获取任务。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击列表中弱点报告获取任务条目后“状态”栏按钮，启用或禁用该弱点报告获取任务。表示弱点报告获取任务状态为已启用，表示弱点报告获取任务状态为禁用。
- 点击列表中弱点报告获取任务条目后的按钮，打开“编辑弱点报告获取任务”页面，编辑所选弱点报告获取任务。
- 点击列表中弱点报告获取任务条目后的按钮，删除所选弱点报告获取任务。如需批量删除弱点报告获取任务，勾选多个弱点报告获取任务条目，点击“删除”按钮。
- 点击“新任务”按钮，创建弱点报告获取任务，详细步骤请参阅新建弱点报告获取任务。
- 点击页面左下角按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角按钮，刷新弱点报告获取任务列表。

新建弱点报告获取任务

创建弱点报告获取任务，请按照以下步骤进行操作：

1. 点击“弱点分析>弱点报告获取任务”。

2. 点击列表右上角“新任务”按钮，打开“新弱点报告获取任务”页面。



在“新弱点报告获取任务”页面，填写弱点报告获取任务基本配置信息。

选项	说明
任务名称（必填项）	指定弱点报告获取任务的名称。
扫描器（必填项）	选择执行弱点报告获取任务的扫描器（已经通过"扫描器配置" 在第173页添加到智源平台）。
任务周期（必填项）	指定弱点报告获取任务的执行周期类型，如每天、每周或每月，并且在下方时间选择框中选择具体执行任务的时间。 例如：选择“每周”，并且在下方指定“星期一”、“08:00:00”，那么在每周星期一的8:00将会执行该弱点报告获取任务。
状态	启用或禁用该弱点报告获取任务。
描述	指定弱点报告获取任务的描述信息。

3. 点击“确定”按钮完成配置。

弱点扫描任务

用户可以在智源平台中配置弱点扫描任务，然后下发到任务指定的被管理的扫描器设备中，被管理的扫描器会按照弱点扫描任务的配置执行扫描任务。

扫描完成后，即可自动从扫描器中获取扫描报告，通过"弱点分析" 在第162页呈现弱点扫描结果。

> **注意:** 目前，弱点扫描任务仅支持下发至山石网科RAS设备。

查看弱点扫描任务

点击“弱点分析>弱点扫描 任务”，打开弱点扫描任务列表页面，查看所有下发的弱点扫描任务。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点扫描任务。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击任务名称，打开扫描任务详情页，查看扫描任务配置信息、任务执行时间、扫描器扫描的资产（扫描任务中扫描的IP地址/段）详细列表。
- 点击列表中弱点扫描任务条目后“状态”栏按钮，启用或禁用该弱点扫描任务。表示弱点扫描任务状态为已启用，表示弱点扫描任务状态为禁用。
- “扫描状态”列展示扫描任务的执行状态，包括空闲、扫描中、扫描完成个数、扫描出错（点击查看出错原因）。
- 状态为空闲、扫描出错、扫描完成的扫描任务，可点击按钮再次启动执行扫描任务；状态为扫描中的扫描任务，可点击按钮终止扫描任务。

- 点击列表中弱点扫描任务条目后的 按钮，打开“编辑弱点扫描任务”页面，编辑所选弱点扫描任务。
- 点击列表中弱点扫描任务条目后的 按钮，删除所选弱点扫描任务。如需批量删除弱点扫描任务，勾选多个弱点扫描任务条目，点击“删除”按钮。
- 点击“新任务”按钮，创建弱点扫描任务，详细步骤请参阅新建弱点扫描任务。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新弱点报告获取任务列表。

新建弱点扫描任务

创建弱点扫描任务，请按照以下步骤进行操作：

1. 点击“弱点分析>弱点扫描任务”。

2. 点击列表右上角“新任务”按钮，打开“新弱点扫描任务”页面。



在“新弱点扫描任务”页面，填写弱点扫描任务基本配置信息。

选项	说明
任务名称（必填项）	指定弱点扫描任务的名称。
扫描器（必填项）	点击下拉菜单选择执行弱点扫描任务的扫描器（已经通过"扫描器配置" 在第173页添加到智源平台）。

选项	说明
扫描类型（必填项）	点击下拉菜单选择扫描器扫描弱点使用的扫描类型，目前仅支持指定为“主机扫描”。
IP地址/段（必填项）	输入扫描器扫描的资产IP地址或IP地址段，然后点击“添加”按钮。
任务周期（必填项）	指定弱点扫描任务的执行周期类型： • 单次扫描：任务配置完成后即可立即执行扫描任务。 • 周期扫描：在每天\每周\每月的指定时间执行扫描任务。在下方“任务执行时间”选择框中选择具体执行任务的时间。 例如：选择“周期扫描”，并且在下方指定“每天”、“08:00:00”，那么在任务配置完成后每天的8:00将会执行该扫描任务。
扫描策略模板（必填项）	扫描策略模板为指定的扫描器中包含的预定义策略模板、自定义策略模板，需要在扫描器设备中配置。根据扫描器的不同，可选择的扫描策略模板也不同。 点击下拉菜单，选择扫描任务要执行的扫描策略模板名称。
扫描配置模板（必填项）	扫描策略模板为指定的扫描器中包含的预定义配置模板、自定义配置模板，需要在扫描器设备中配置。根据扫描器的不同，可选择的扫描配置模板也不同。 点击下拉菜单，选择扫描任务要执行的扫描配置模板名称。
描述	指定弱点扫描任务的描述信息。

3. 点击“确定”按钮完成配置，新创建的弱点扫描任务将会自动立即启用。

扫描器配置

扫描器配置页面用于配置并管理添加到智源平台的扫描器。

查看扫描器列表

点击“弱点分析>扫描器配置”，打开扫描器列表页面。



- 点击“新扫描器”按钮，添加一个新的扫描器到智源平台。具体步骤请参阅添加扫描器。
- 点击指定扫描器部分的按钮，打开编辑页面，编辑所选扫描器的参数信息。在该页面，点击“编辑”按钮，编辑所选扫描器；点击“测试”按钮，测试所选扫描器的连通性；点击“取消”按钮，关闭该页面。
- 点击指定扫描器部分的按钮，打开“扫描器详情”页面，查看扫描器名称、IP地址、类型、端口、登录信息等参数。在该页面，点击“编辑”按钮，编辑所选扫描器；点击“测试”按钮，测试所选扫描器的连通性；点击“取消”按钮，关闭该页面。
- 点击指定扫描器部分的按钮，删除指定扫描器。
- 如需删除所有扫描器，点击右上角“全选” 复选框，然后点击“删除”按钮；如需批量删除部分扫描器，点击指定扫描器部分右上角的复选框，然后点击“删除”按钮。

添加扫描器

添加新的扫描器，请按照以下步骤进行操作：

1. 点击“弱点分析>扫描器配置”，打开扫描器列表页面。

2. 点击“新扫描器”按钮，打开<新扫描器>页面。



在“新扫描器”页面，填写扫描器基本配置信息。

选项	说明
扫描器名称（必填项）	指定扫描器的名称。
IP地址（必填项）	指定扫描器的IP地址。

选项	说明
端口（必填项）	指定扫描器的端口号。默认端口号为8834。
类型	指定扫描器的类型。目前，支持添加Nessus扫描器或者山石网科RAS设备。
登录信息	指定登录扫描器的账号和密码。 1. 点击“新增”按钮，在文本框中输入登录账号和对应账号的密码。 2. 如需添加多个登录信息，重复步骤1的操作。 3. 如需删除登录信息，勾选登录信息条目前的复选框，然后点击下方“删除”按钮。
描述	指定扫描器的描述信息。

3. 点击“确定”按钮完成配置。
4. 点击“测试”按钮，测试所选扫描器的连通性。
5. 点击“取消”按钮，关闭该页面。

弱点分析配置案例

本节介绍智源平台弱点分析功能的典型配置示例。

组网场景

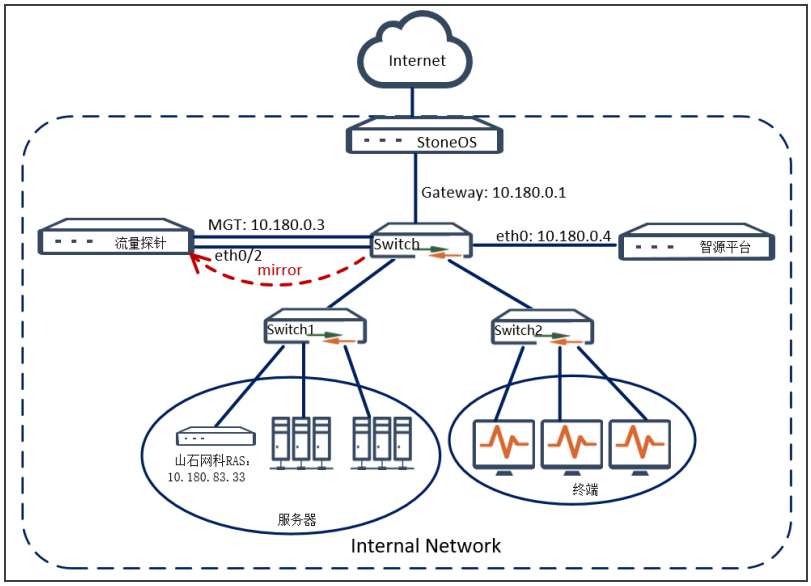
按照智源的典型部署将智源平台和流量探针部署在用户内网环境中，威胁溯源插件部署在用户服务器或终端上。智源平台接收来自流量探针、山石网科安全设备以及用户服务器或终端的信息，从而对全网进行监控和分析。

该案例包含以下两种场景：

- 山石网科RAS设备（IP：10.180.83.33）作为弱点扫描器，在智源平台上使用弱点分析功能，配置下发至山石网科RAS设备的弱点扫描任务：每周五10:00在扫描器上对指定的内网所有资产（IP地址段：10.180.80.61-10.180.80.65）进行弱点扫描，扫描完成后获取弱点扫描结果。
- 用户在某服务器（IP：10.180.83.34）上安装了系统漏洞扫描与分析软件（Nessus软件），使之成为弱点扫描器，并且在该扫描器上指定扫描任务周期为每天2点。在智源平台上配置弱点报告获取任务，每天8:00获取该扫描器上对当前内网所有资产的扫描结果；

通过该功能重点对风险资产的安全脆弱性（弱点）进行全面检测，对发现的弱点进一步下发工单实施处理。

典型部署组网图如下图：



准备工作

在配置前，请确保完成以下准备工作：

- 已根据典型部署完成部署，具体步骤可参阅"第1章 部署智源" 在第2页章节或者《山石网科智源智能安全运营系统部署手册》。
- 确保智源平台已经接收到流量探针、山石安全设备以及服务器/终端的Sysmon数据信息。
- 已部署完成山石网科RAS设备。
- 确保智源平台的“山石弱点情报库”已升级到最新版本。

配置步骤

步骤一：扫描器准备工作。

- 山石网科RAS设备中已配置完成扫描策略模板以及扫描配置模板，具体方法请参阅“山石网科远程安全评估系统”相关手册。
- 在服务器上安装系统漏洞扫描与分析软件（Nessus软件），具体安装方法请参阅Nessus软件相关手册。

步骤二：在智源平台上添加扫描器。

添加山石网科RAS设备作为扫描器：

选择“弱点分析>扫描器配置”，并点击“新扫描器”按钮。

在“新扫描器”页面，配置如下：

- 扫描器名称：山石网科RAS设备
- 类型：山石网科RAS
- IP地址：10.180.83.33
- 端口：8834
- 登录信息：登录账号hillstone，密码hillstone



步骤二：在智源平台上添加扫描器。

添加Nessus扫描器：

选择“弱点分析>扫描器配置”，并点击“新扫描器”按钮。

在“新扫描器”页面，配置如下：

- 扫描器名称：Nessus扫描器
- 类型：Nessus
- IP地址：10.180.83.34
- 端口：8834
- 登录信息：登录账号admin，密码admin



步骤三：创建下发至山石网科RAS设备的弱点扫描任务。

选择“弱点分析>弱点扫描任务”，并点击“新任务”按钮。

在“新弱点扫描任务”页面，配置如下：

- 任务名称：山石网科RAS设备扫描任务
- 扫描器：山石网科RAS设备
- 扫描类型：主机扫描
- IP地址/段：10.180.80.61-10.180.80.65
- 任务周期：周期扫描
- 任务执行时间：每周，星期五，10:00:00
- 扫描策略模板：Ubuntu
- 扫描配置模板：快速扫描



步骤四：创建弱点报告获取任务，每天8:00从Nessus扫描器中获取弱点报告。

选择“弱点分析>弱点报告获取”，然后点击列表右上角“新任务”按钮。

在“新弱点报告获取”页面，配置如下：

- 任务名称：Nessus报告
- 扫描器：选择“Nessus扫描器”
- 任务周期：选择“每天”，“08:00:00”
- 状态：开启



步骤五：导入本地弱点报告（可选）。

选择“弱点分析>弱点分析”，然后点击页面右上角 导入 按钮。在“导入报告”页面，配置如下：

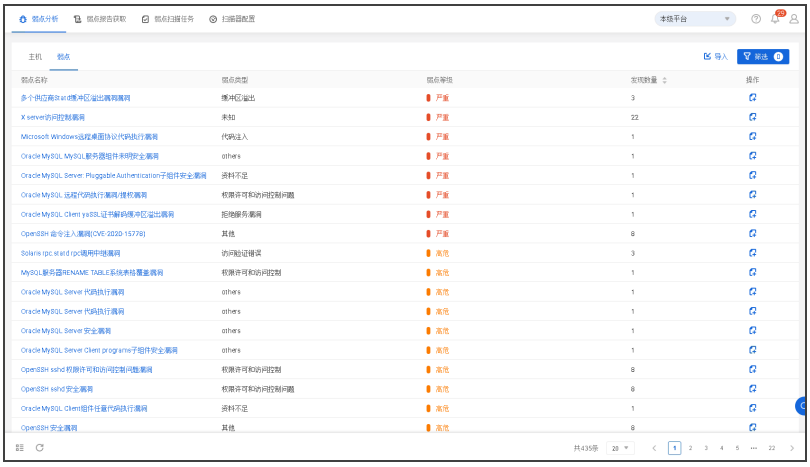
- 报告文件：按需导入本地弱点报告文件（.nessus文件）



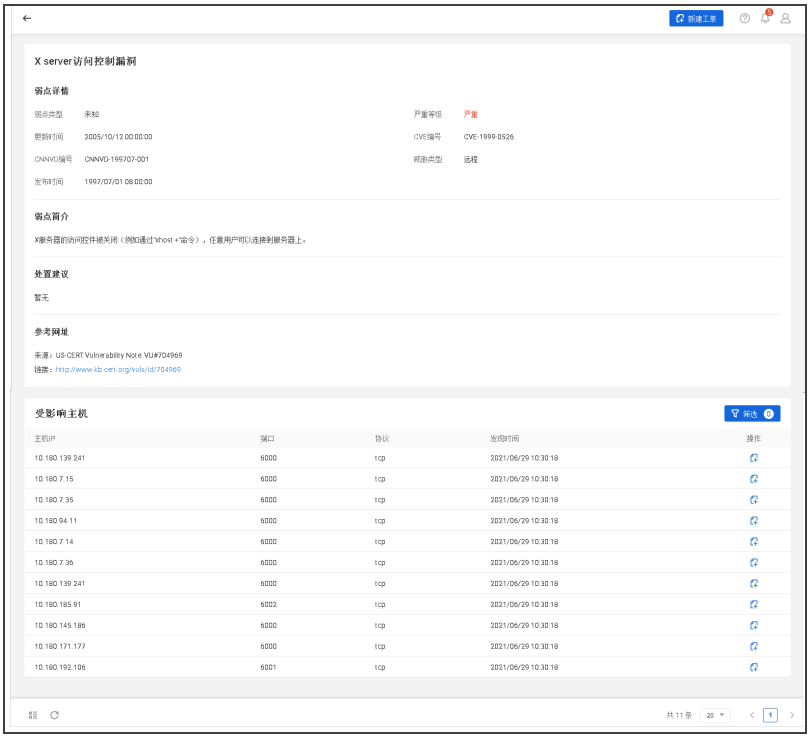
步骤六：查看弱点分析结果。

选择“弱点分析>弱点分析>弱点”。

在弱点列表页面，查看发现的内网资产存在的所有弱点。



点击某一弱点名称链接，如“OpenSSH CBC模式信息泄露漏洞”打开该弱点的详情页面，查看该弱点详细信息、简介、处置建议、参考网站以及受影响的主机列表。



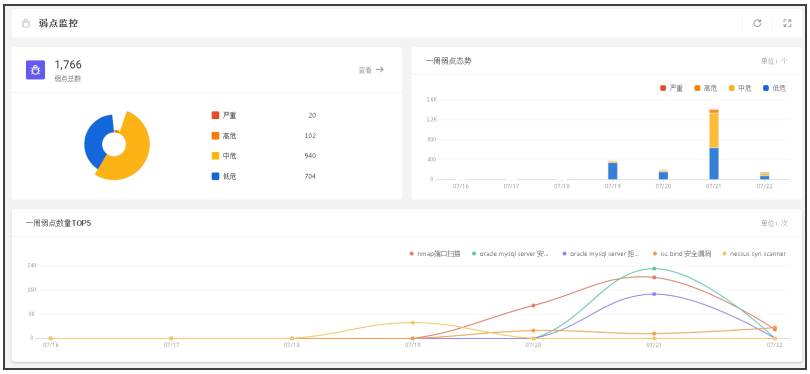
步骤七：针对发现的弱点，新建工单进行响应处理。

选择“弱点分析>弱点分析>弱点”，选择需要处理的弱点，然后点击该弱点条目后的按钮，新建工单对发现的弱点进行进一步响应处理。



步骤八：在“态势监控”中查看弱点的态势、数量等统计内容。

选择“态势监控”，查看所有弱点的分布统计结果、一周弱点态势、以及一周弱点数量TOP5。



第5章 风险管理

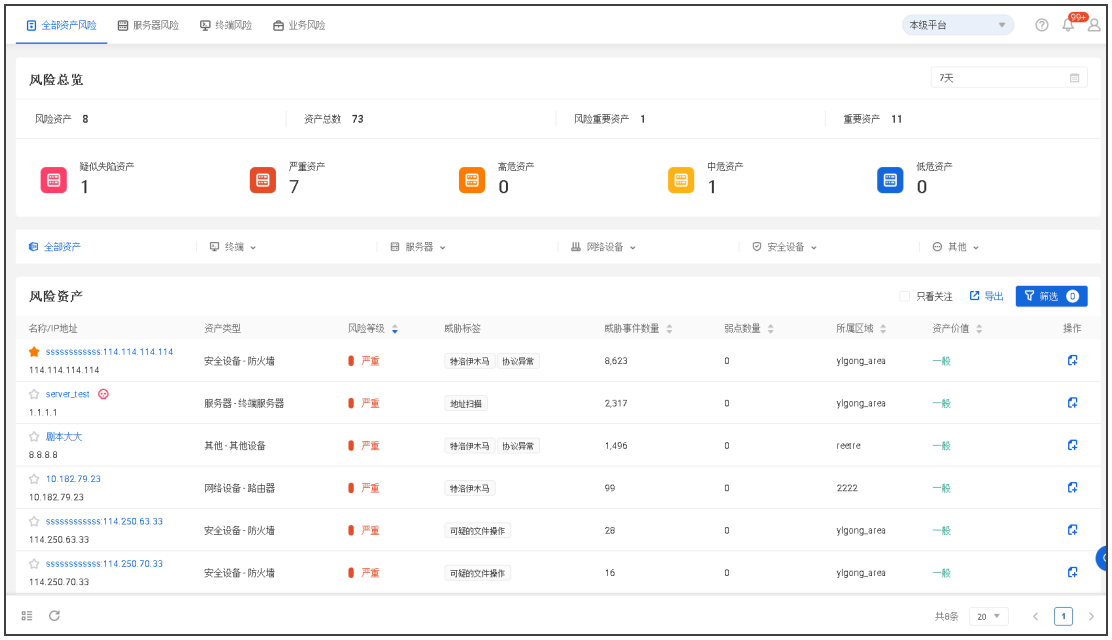
风险管理页面以内网资产为核心，配合"第3章 威胁分析" 在第114页、"第4章 弱点分析" 在第160页功能，从威胁、脆弱性（弱点）、资产价值几方面综合展示所有服务器、终端以及业务的风险状态。

风险管理部分包含如下内容：

- "全部资产风险" 在第185页：整体展示所有风险资产，介绍如何查看风险资产列表和详情。
- "服务器风险" 在第194页：介绍服务器风险总览内容、如何查看风险服务器列表和详情。
- "终端风险" 在第203页：介绍终端风险总览内容、如何查看风险终端列表和详情。
- "业务风险" 在第212页：介绍业务风险总览内容、如何查看风险业务列表和详情。

全部资产风险

点击“风险管理 > 全部资产风险”，打开全部资产风险页面，展示资产的安全风险状态总览以及所有风险资产详情列表。



风险状态总览

最上方展示资产的数量统计，包括风险资产个数、资产总数、风险重要资产个数以及重要资产个数。

- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的全部风险资产信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的全部风险资产信息。当选择下级平台时，支持查看和导出全部风险资产信息，不支持新建工单、添加关注资产等操作。
- 选择风险发生的时间范围，符合条件的风险资产信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击“风险资产”的数字，刷新下方“风险资产”列表，查看所有风险资产列表详细信息。

- 点击“资产总数”的数字跳转至资产列表页面，或者点击“Ctrl+鼠标左键”在新标签页中打开资产列表页面，查看资产列表详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击“风险重要资产”的数字，在下方“风险资产 ”列表查看资产价值为“重要”的风险资产详细信息。
- 点击“重要资产”的数字跳转至资产列表页面，或者点击“Ctrl+鼠标左键”在新标签页中打开资产列表页面，查看资产价值为“重要”的资产详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击各级别资产对应的数字，在下方“风险资产 ”列表查看不同风险等级的风险资产详细信息。
- 点击资产类型，在下方“风险资产”列表查看指定类型风险资产的详细信息。

风险资产

页面下方展示风险资产列表。

- 点击“导出”按钮，以CSV格式导出系统存储的前10000个风险资产信息或者筛选、排序后的前10000个风险资产信息。
- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的风险资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 点击列表中具体资产前的 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”前的复选框，列表中将展示所有被设为重点关注的资产。
- 点击列表中风险资产条目后的按钮，或者在风险资产详情页面点击“新建工单”按钮，配置对应的工单对风险资产进行响应。
- 点击资产名称链接，打开所选风险资产的详情页面，查看风险资产详情。

- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新风险资产列表。

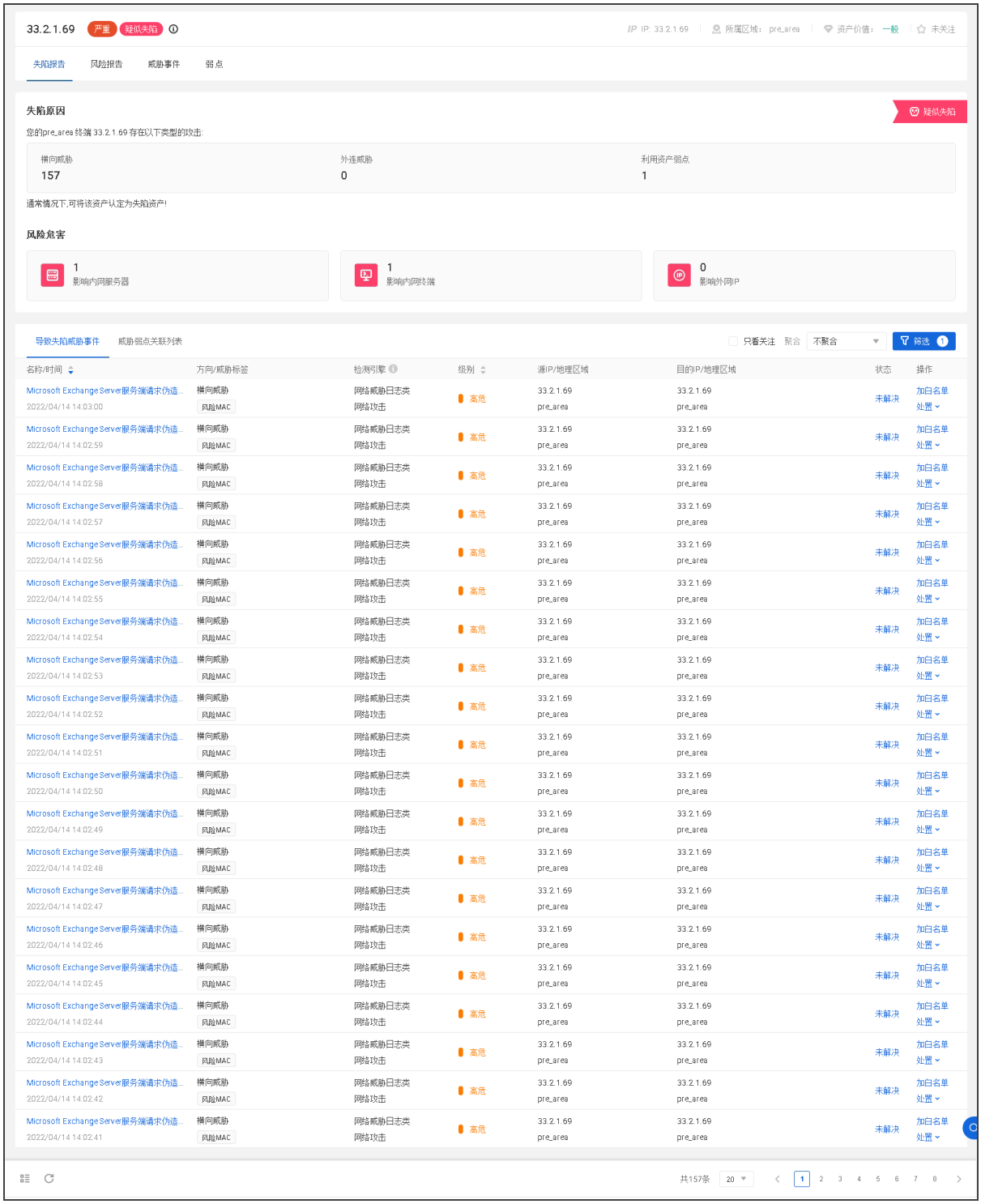
查看风险资产详情

在风险资产详细信息页面，从失陷报告、风险报告、威胁事件、弱点四方面查看所选风险资产详细信息。

若需查看所选风险资产在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。

失陷报告

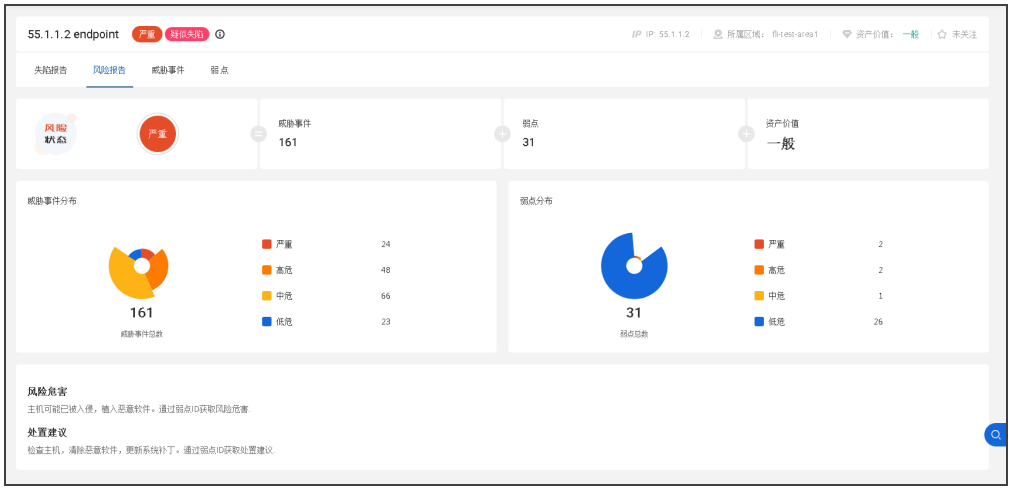
风险资产详情页面<失陷报告>标签页展示失陷原因、风险危害、导致失陷的威胁事件列表以及威胁弱点关联列表。



- 鼠标悬停在风险资产IP地址旁ⓘ处，查看失陷评估的时间。
- **失陷原因**：从横向威胁、外连威胁、利用资产弱点数量展示失陷的原因。

- **风险危害**：展示该风险资产影响到的其他内网服务器、内网终端数量，以及影响到外网的IP数量。
- **导致失陷威胁事件**：展示导致该风险资产失陷的威胁事件详细列表。点击威胁事件名称，打开威胁事件详情页面，查看所选威胁事件的详细信息。勾选“只看关注”复选框，仅查看设为关注的威胁事件。
- **威胁弱点关联列表**：展示导致失陷的威胁事件利用的弱点详细列表。

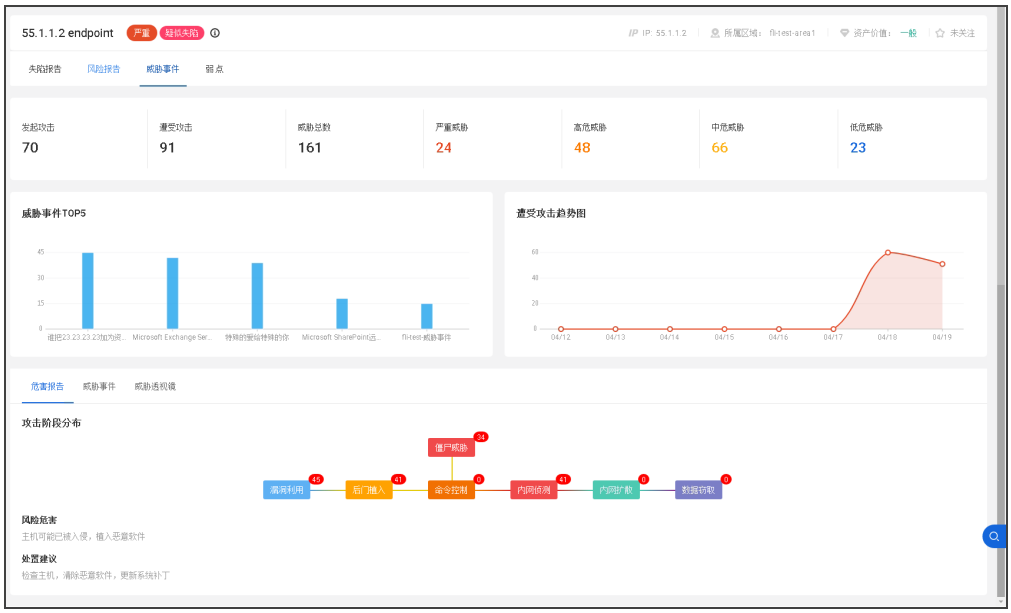
风险报告



- 上方从威胁事件数量、弱点数量、资产价值来综合展示风险资产级别的统计结果。
  - 点击威胁事件对应的数字，可跳转至威胁事件标签页，查看威胁事件列表详细信息。
  - 点击弱点对应的数字，可跳转至弱点标签页，查看弱点列表详细信息。
- **威胁事件分布**：玫瑰图展示所选风险资产发现的未解决威胁事件的分布统计结果，下方展示威胁事件总数，右侧展示各级别的威胁事件数量。
  - 点击右侧各级别图例或对应的数字，图例变灰色，取消所选级别在玫瑰图的统计展示。
  - 鼠标悬停在玫瑰图各部分，显示对应级别的威胁事件数量。
  - 点击玫瑰图各部分，可跳转至威胁事件标签页，查看对应级别的威胁事件列表详细信息。

- **弱点分布**：玫瑰图展示所选风险资产上发现的弱点的分布统计结果，下方展示弱点总数，右侧展示各弱点等级的弱点数量。
    - 点击右侧各弱点等级图例或对应的数字，图例变灰色，取消所选弱点等级在玫瑰图的统计展示。
    - 鼠标悬停在玫瑰图各部分，显示对应级别的弱点数量。
    - 点击玫瑰图各部分，可跳转至弱点标签页，查看对应弱点等级的弱点列表详细信息。
- 最下方展示所选风险资产的风险危害描述，以及针对该风险资产的风险状态提供的处置建议。

威胁事件

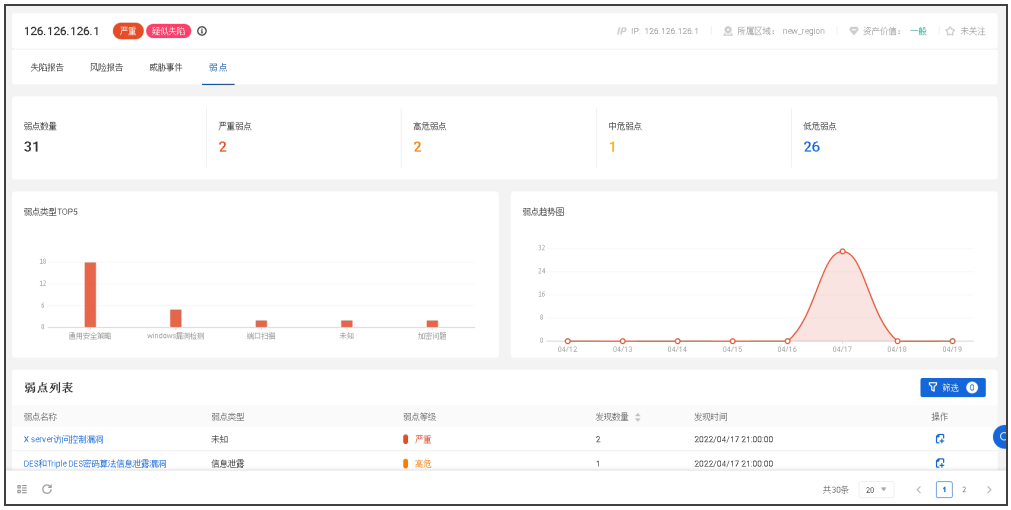


- 上方概览展示所选风险资产发生的威胁事件总数、发起攻击的次数、被攻击的次数，以及各级别威胁事件的数量。
    - 点击威胁总数对应的数字，系统将根据状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击发起攻击对应的数字，系统将根据源IP地址和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。

    - 点击遭受攻击对应的数字，系统将根据目的IP地址和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- **威胁事件TOP5**：以柱状图形式展示所选风险资产指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- **遭受攻击趋势图**：以曲线图的方式展示所选风险资产指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选风险资产发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内所选风险资产发生的未解决威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”前的复选框，列表中将展示所有被设为关注的威胁事件。
- **威胁透视镜**：以图标和箭头连接线的形式展示指定时间周期内所选风险资产发生的威胁事件的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。
    - 点击上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。

弱点

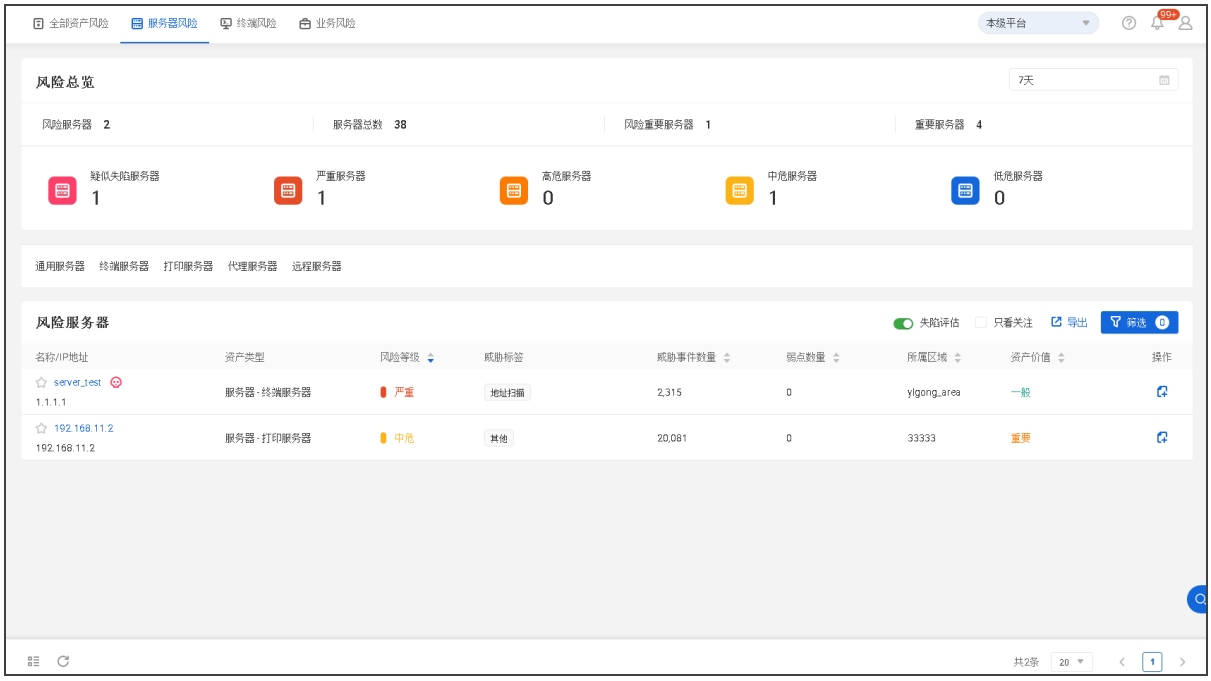


- 上方概览展示所选风险资产存在的弱点总数、各级别弱点的数量。
    - 点击弱点数量对应的数字，系统将全部的弱点显示在页面下方的弱点列表中。
    - 点击各弱点等级对应的数字，系统将根据弱点等级作为筛选条件筛选对应的弱点，显示在页面下方的弱点列表中。
- **弱点类型TOP5**：以柱状图形式展示所选风险资产指定时间内存在的数量排名前5的弱点类型。
    - 鼠标悬停在柱状图上，显示对应类型弱点的数量。
- **弱点趋势图**：以曲线图的方式展示所选风险资产指定时间内弱点数量的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点弱点的数量。
- 下方列表展示所选风险资产存在的所有弱点。
    - 点击上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
    - 点击弱点列表中弱点条目后的按钮，或者在弱点详情页面点击“新建工单”按钮，配置对应的工单对弱点进行响应。

- 点击弱点名称链接，打开所选弱点的详情页面，查看该弱点详细信息、简介、处置建议、参考网站以及受影响的主机列表。

服务器风险

点击“风险管理 > 服务器风险”，打开服务器风险页面，展示服务器的安全风险状态总览以及所有风险服务器详情列表。



风险状态总览

最上方展示服务器的数量统计，包括风险服务器个数、服务器总数、风险重要服务器个数以及重要服务器个数。

- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的风险服务器信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的风险服务器信息。当选择下级平台时，支持查看和导出风险服务器信息，不支持新建工单操作、启用/禁用失陷评估、添加关注资产等操作。
- 选择风险发生的时间范围，符合条件的风险服务器信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。

- 点击“风险服务器”的数字，刷新下方“风险服务器 ”列表，查看所有风险服务器列表详细信息。
- 点击“服务器总数”的数字跳转至资产列表页面，或者点击“Ctrl+鼠标左键”在新标签页中打开资产列表页面，查看服务器列表详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击“风险重要服务器”的数字，在下方“风险服务器 ”列表查看资产价值为“重要”的风险服务器详细信息。
- 点击“重要服务器”的数字跳转至资产列表页面，或者点击“Ctrl+鼠标左键”在新标签页中打开资产列表页面，查看资产价值为“重要”的服务器列表详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击各级别服务器对应的数字，在下方“风险服务器 ”列表查看不同风险等级的风险服务器详细信息。如未开启失陷评估功能，“疑似失陷服务器”处将显示“未评估” 。
- 点击服务器子类，在下方“风险服务器 ”列表查看服务器不同子类下的风险服务器详细信息。

风险服务器

页面下方展示风险服务器列表。

- 失陷评估：点击“失陷评估”的启用按钮，开启失陷评估功能，开启后，系统通过资产相关的威胁事件、威胁关联的弱点多方面将对资产进行失陷评估，并给出判定结论和失陷原因。默认情况下，服务器失陷评估功能为开启状态。
- 点击列表中具体资产前的 ☆ 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”前的复选框，列表中将展示所有被设为重点关注的资产。
- 点击“导出”按钮，以CSV格式导出系统存储的前10000个风险服务器信息或者筛选、排序后的前10000个风险服务器信息。

- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的风险服务器。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 点击列表中风险服务器条目后的按钮，或者在风险服务器详情页面点击“新建工单”按钮，配置对应的工单对风险服务器进行响应。
- 点击服务器名称链接，打开所选风险服务器的详情页面，查看风险服务器详情。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新风险服务器列表。

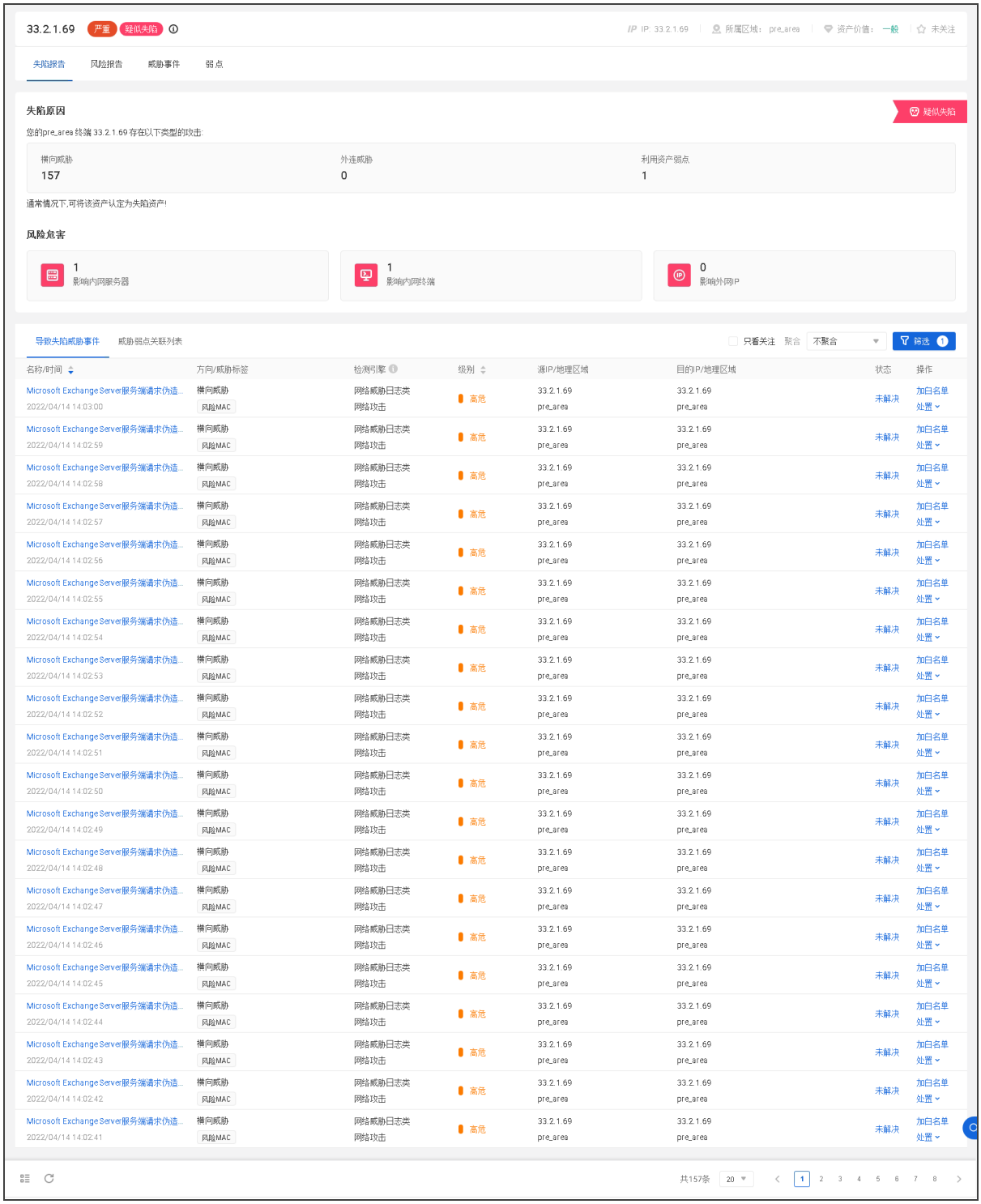
查看风险服务器详情

在风险服务器详细信息页面，从失陷报告、风险报告、威胁事件、弱点四方面查看所选风险服务器详细信息。

若需查看所选风险服务器在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。

失陷报告

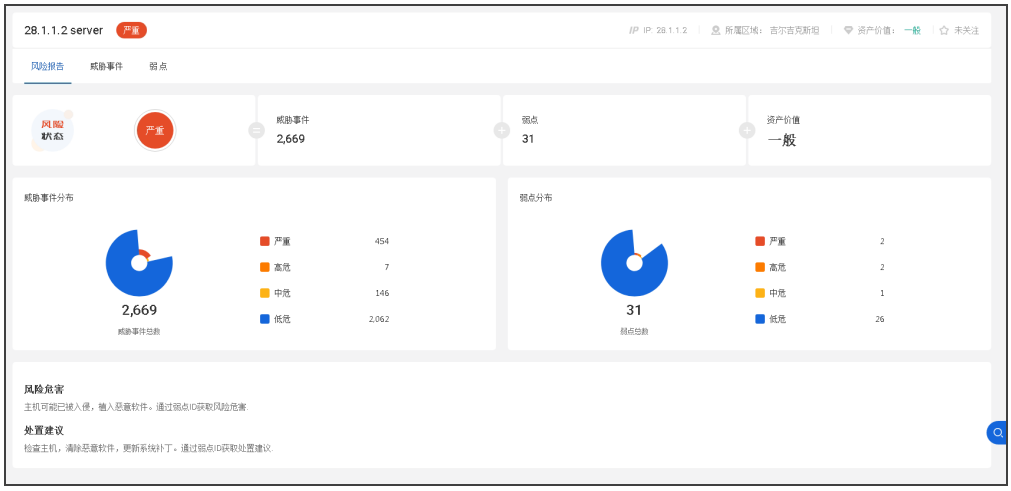
当开启“失陷评估”功能后，风险服务器详情页面<失陷报告>标签页可展示失陷原因、风险危害、导致失陷的威胁事件列表以及威胁弱点关联列表。



- 鼠标悬停在风险服务器IP地址旁ⓘ处，查看失陷评估的时间。
- **失陷原因**：从横向威胁、外连威胁、利用资产弱点数量展示失陷的原因。

- **风险危害**：展示该风险服务器影响到的其他内网服务器、内网终端数量，以及影响到外网的IP数量。
- **导致失陷威胁事件**：展示导致该风险服务器失陷的威胁事件详细列表。点击威胁事件名称，打开威胁事件详情页面，查看所选威胁事件的详细信息。勾选“只看关注”复选框，仅查看设为关注的威胁事件。
- **威胁弱点关联列表**：展示导致失陷的威胁事件利用的弱点详细列表。

风险报告



- 上方从威胁事件数量、弱点数量、资产价值来综合展示风险服务器级别的统计结果。
  - 点击威胁事件对应的数字，可跳转至威胁事件标签页，查看威胁事件列表详细信息。
  - 点击弱点对应的数字，可跳转至弱点标签页，查看弱点列表详细信息。
- **威胁事件分布**：玫瑰图展示所选风险服务器上发现的未解决威胁事件的分布统计结果，下方展示威胁事件总数，右侧展示各级别的威胁事件数量。
  - 点击右侧各级别图例或对应的数字，图例变灰色，取消所选级别在玫瑰图的统计展示。
  - 鼠标悬停在玫瑰图各部分，显示对应级别的威胁事件数量。
  - 点击玫瑰图各部分，可跳转至威胁事件标签页，查看对应级别的威胁事件列表详细信息。

- **弱点分布**：玫瑰图展示所选风险服务器上发现的弱点的分布统计结果，下方展示弱点总数，右侧展示各弱点等级的弱点数量。
    - 点击右侧各弱点等级图例或对应的数字，图例变灰色，取消所选弱点等级在玫瑰图的统计展示。
    - 鼠标悬停在玫瑰图各部分，显示对应级别的弱点数量。
    - 点击玫瑰图各部分，可跳转至弱点标签页，查看对应弱点等级的弱点列表详细信息。
- 最下方展示所选风险服务器的风险危害描述，以及针对该风险服务器的风险状态提供的处置建议。

威胁事件

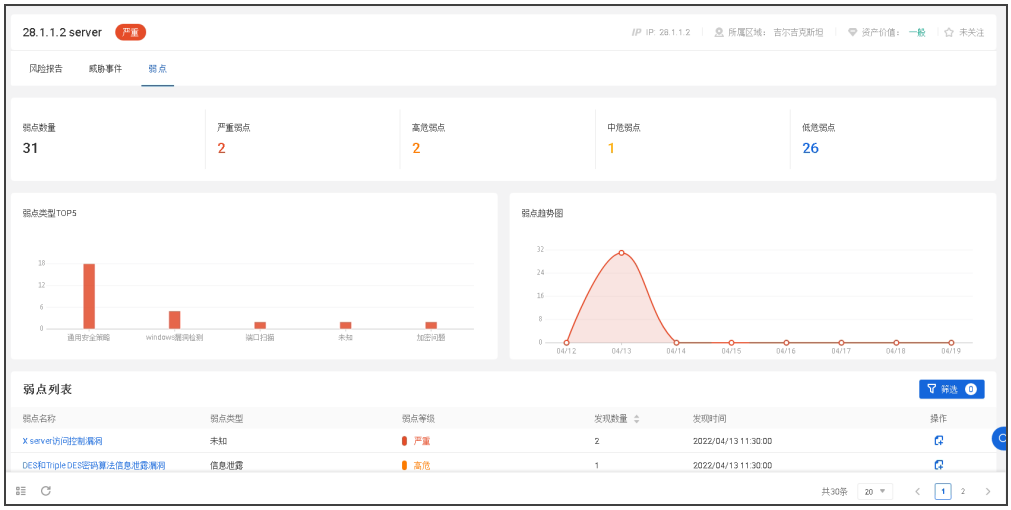


- 上方概览展示所选风险服务器发生的威胁事件总数、发起攻击的次数、被攻击的次数，以及各级别威胁事件的数量。
    - 点击威胁总数对应的数字，系统将根据状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击发起攻击对应的数字，系统将根据源IP地址和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。

    - 点击遭受攻击对应的数字，系统将根据目的IP地址和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- **威胁事件TOP5**：以柱状图形式展示所选风险服务器指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- **遭受攻击趋势图**：以曲线图的方式展示所选风险服务器指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选风险服务器发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内所选风险服务器发生的未解决威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示被设为关注的威胁事件。
- **威胁透视镜**：以图标和箭头连接线的形式展示指定时间周期内所选风险服务器发生的威胁事件的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。
    - 点击上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。

弱点

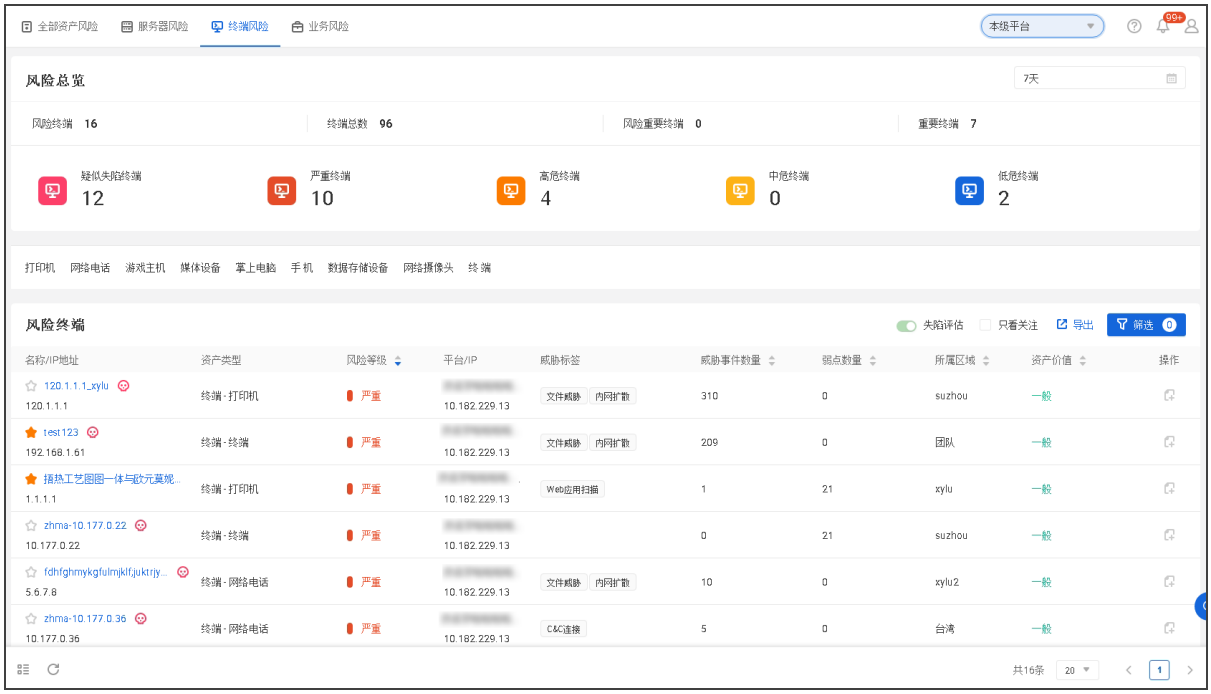


- 上方概览展示所选风险服务器存在的弱点总数、各级别弱点的数量。
  - 点击弱点数量对应的数字，系统将全部的弱点显示在页面下方的弱点列表中。
  - 点击各弱点等级对应的数字，系统将根据弱点等级作为筛选条件筛选对应的弱点，显示在页面下方的弱点列表中。
- **弱点类型TOP5**：以柱状图形式展示所选风险服务器存在的数量排名前5的弱点类型。
  - 鼠标悬停在柱状图上，显示对应类型弱点的数量。
- **弱点趋势图**：以曲线图的方式展示所选风险服务器指定时间内弱点数量的变化趋势。
  - 鼠标悬停在曲线图指定位置上，显示对应时间点弱点的数量。
- 下方列表展示所选风险服务器存在的所有弱点列表。
  - 点击上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
  - 点击弱点列表中弱点条目后的按钮，或者在弱点详情页面点击“新建工单”按钮，配置对应的工单对弱点进行响应。

- 点击弱点名称链接，打开所选弱点的详情页面，查看该弱点详细信息、简介、处置建议、参考网站以及受影响的主机列表。

终端风险

点击“风险管理 > 终端风险”，打开终端风险页面，展示终端的安全风险状态总览以及所有风险终端详情列表。



风险状态总览

最上方展示终端的数量统计，包括即风险终端个数、终端总数、风险重要终端个数以及重要终端个数。

- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的风险终端信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的风险终端信息。当选择下级平台时，支持查看和导出风险终端信息，不支持新建工单操作、启用/禁用失陷评估、添加关注资产等操作。
- 选择风险发生的时间范围，符合条件的风险终端信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。

- 点击“风险终端”，刷新下方“风险终端”列表，查看所有风险终端列表详细信息。
- 点击“终端总数”的数字跳转至资产列表页面，或者点击“Ctrl+鼠标左键”在新标签页中打开资产列表页面，查看终端列表详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击“风险重要终端”的数字，在下方“风险终端”列表查看资产价值为“重要”的风险终端详细信息。
- 点击“重要终端”的数字跳转至资产列表页面，或者点击“Ctrl+鼠标左键”在新标签页中打开资产列表页面，查看资产价值为“重要”的终端详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击各级别终端对应的数字，在下方“风险终端”列表查看不同风险等级的风险终端详细信息。如未开启失陷评估功能，“疑似失陷终端”处将显示“未评估”。

风险终端

页面下方展示风险终端列表。

- 失陷评估：点击“失陷评估”的启用按钮，开启失陷评估功能，开启后，系统通过资产相关的威胁事件、威胁关联的弱点多方面将对资产进行失陷评估，并给出判定结论和失陷原因。默认情况下，终端失陷评估功能为关闭状态。
- 点击列表中具体资产前的 ☆ 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”前的复选框，列表中将展示所有被设为重点关注的资产。
- 点击“导出”按钮，以CSV格式导出系统存储的前10000个风险终端信息或者筛选、排序后的前10000个风险终端信息。
- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的风险终端。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 点击列表中风险终端条目后的  按钮，或者在风险终端详情页面点击“新建工单”按钮，配置对应的工单对风险终端进行响应。

- 点击终端名称链接，打开所选风险终端的详情页面，查看风险终端详情。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新风险终端列表。

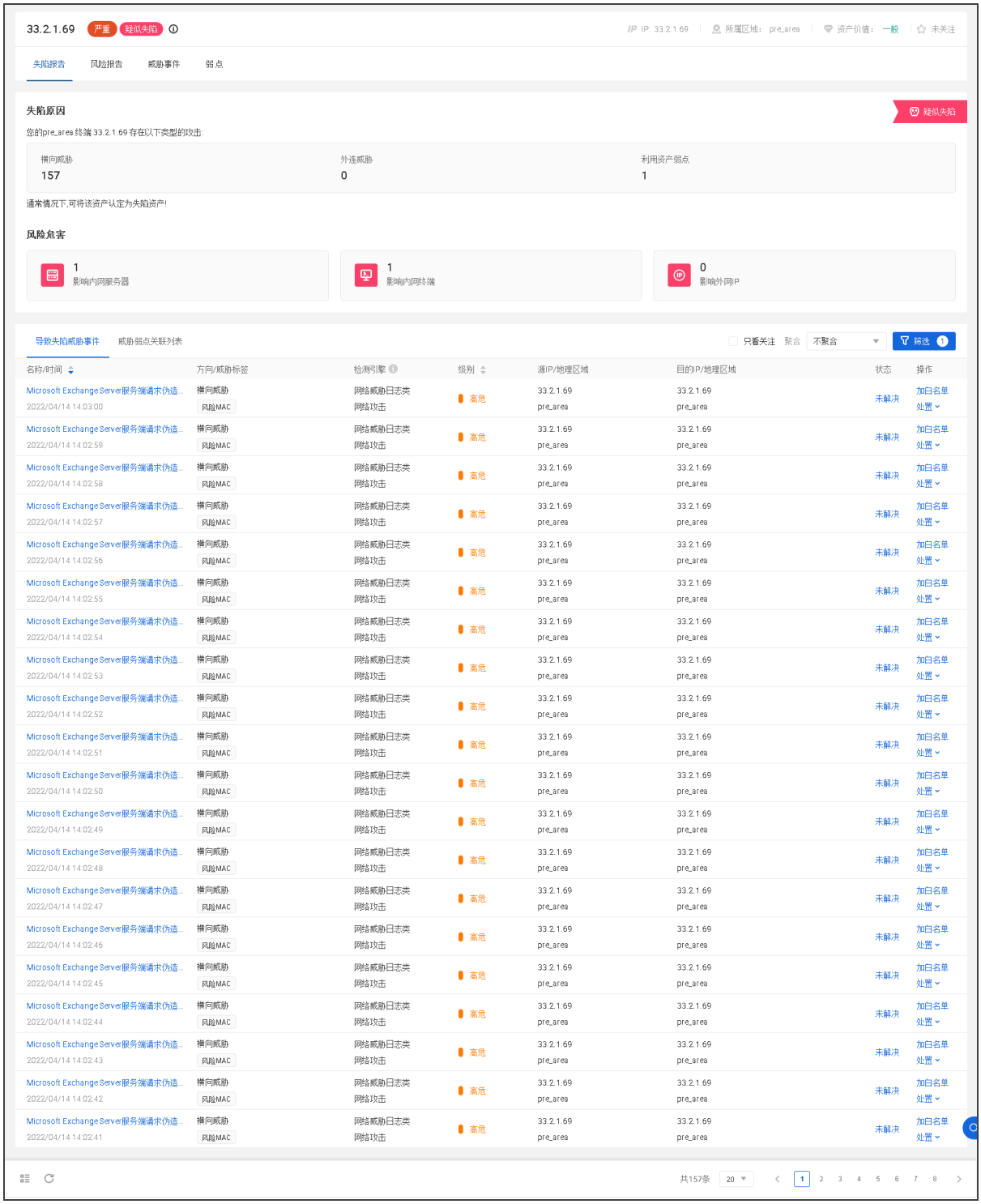
查看风险终端详情

在风险终端详细信息页面，从失陷报告、风险报告、威胁事件、弱点四方面查看所选风险终端详细信息。

若需查看所选风险终端在某个时间范围内的详细信息，在页面右上角选择具体的开始时间和结束时间或者可直接点击“1小时/12小时/24小时/7天/30天”，符合指定时间范围内的详细信息将展示在页面中。

失陷报告

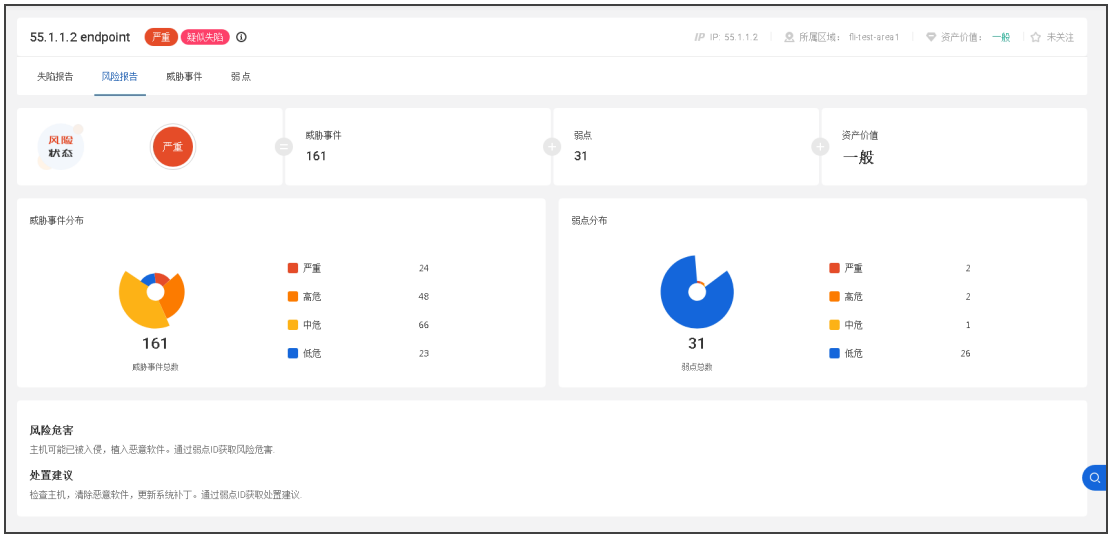
当开启“失陷评估”功能后，风险终端详情页面<失陷报告>标签页可展示失陷原因、风险危害、导致失陷的威胁事件列表以及威胁弱点关联列表。



- 鼠标悬停在风险终端IP地址旁ⓘ处，查看失陷评估的时间。
- **失陷原因**：从横向威胁、外连威胁、利用资产弱点数量展示失陷的原因。

- **风险危害**：展示该风险服务器影响到的其他内网服务器、内网终端数量，以及影响到外网的IP数量。
- **导致失陷威胁事件**：展示导致该风险终端失陷的威胁事件详细列表。点击威胁事件名称，打开威胁事件详情页面，查看所选威胁事件的详细信息。勾选“只看关注”复选框，仅查看设为关注的威胁事件。
- **威胁弱点关联列表**：展示导致失陷的威胁事件利用的弱点详细列表。

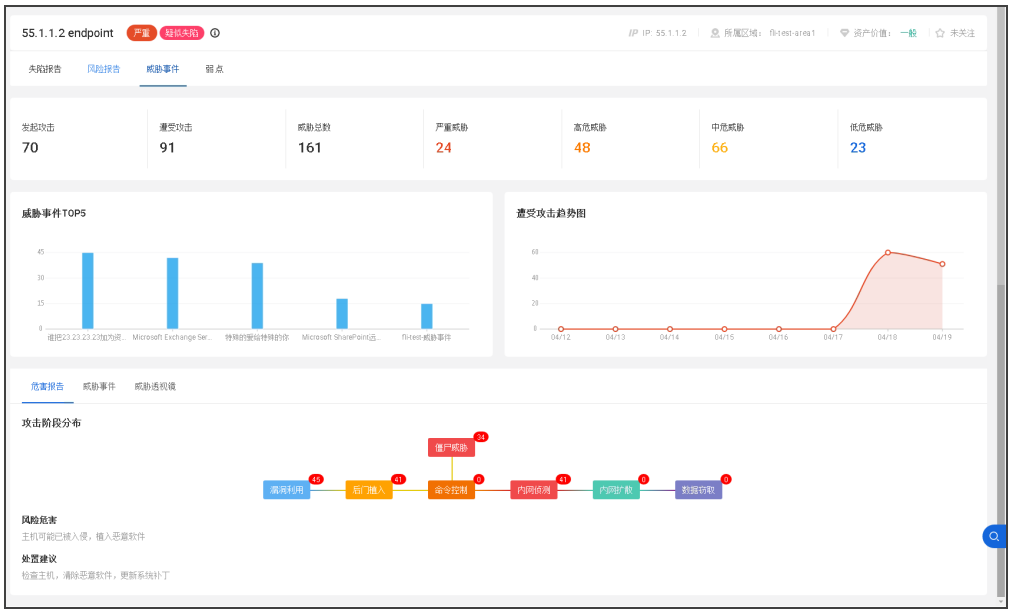
风险报告



- 上方从威胁事件数量、弱点数量、资产价值来综合展示风险终端级别的统计结果。
  - 点击威胁事件对应的数字，可跳转至威胁事件标签页，查看威胁事件列表详细信息。
  - 点击弱点对应的数字，可跳转至弱点标签页，查看弱点列表详细信息。
- **威胁事件分布**：玫瑰图展示所选风险终端上发现的未解决威胁事件的分布统计结果，下方展示威胁事件总数，右侧展示各级别的威胁事件数量。
  - 点击右侧各级别图例或对应的数字，图例变灰色，取消所选级别在玫瑰图的统计展示。
  - 鼠标悬停在玫瑰图各部分，显示对应级别的威胁事件数量。
  - 点击玫瑰图各部分，可跳转至威胁事件标签页，查看对应级别的威胁事件列表详细信息。

- **弱点分布**：玫瑰图展示所选风险终端上发现的弱点的分布统计结果，下方展示弱点总数，右侧展示各级别的弱点数量。
    - 点击右侧各弱点等级图例或对应的数字，图例变灰色，取消所选弱点等级在玫瑰图的统计展示。
    - 鼠标悬停在玫瑰图各部分，显示对应级别的弱点数量。
    - 点击玫瑰图各部分，可跳转至弱点标签页，查看对应级别的弱点列表详细信息。
- 最下方展示所选风险终端的风险危害描述，以及针对该风险终端的风险状态提供的处置建议。

威胁事件

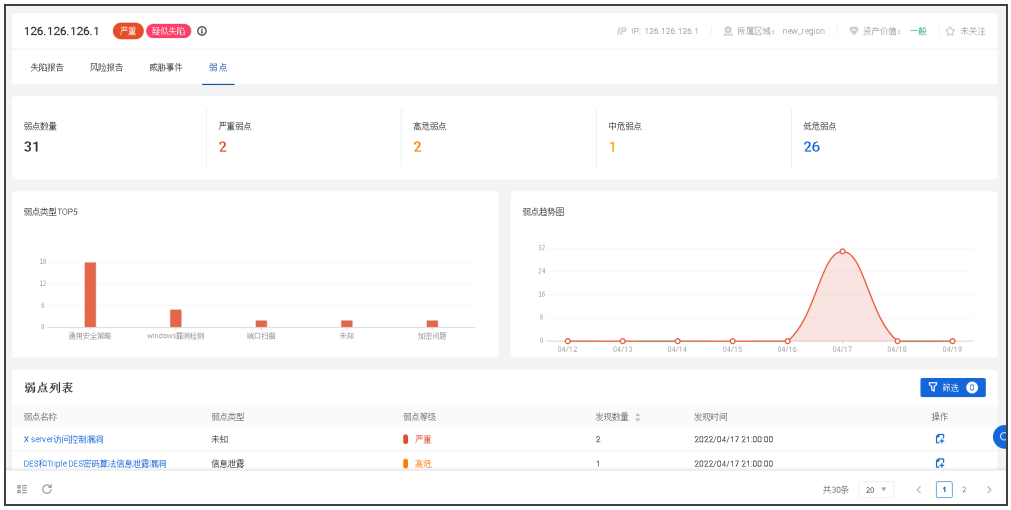


- 上方概览展示所选风险终端发生的未解决威胁事件总数、发起攻击的次数、被攻击的次数，以及各级别威胁事件的数量。
    - 点击威胁总数对应的数字，系统将根据状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击发起攻击对应的数字，系统将根据源IP地址和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。

    - 点击遭受攻击对应的数字，系统将根据目的IP地址和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
    - 点击各级别威胁对应的数字，系统将根据级别和状态作为筛选条件筛选对应的威胁事件，显示在页面下方<威胁事件>标签页的威胁事件列表中。
- **威胁事件TOP5**：以柱状图形式展示所选风险终端指定时间内发生的数量排名前5的威胁事件。
    - 鼠标悬停在柱状图上，显示对应威胁事件的数量。
- **遭受攻击趋势图**：以曲线图的方式展示所选风险终端指定时间内被攻击次数的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点被攻击的威胁事件的数量。
- **危害报告**：展示指定时间周期内所选风险终端发生威胁事件的攻击阶段分布，并描述风险危害以及处置建议。各攻击阶段右上角数字表示处于该阶段的威胁事件数量。
- **威胁事件**：以列表的方式展示指定时间周期内所选风险终端发生的未解决威胁事件。具体操作，参见事件列表。勾选列表上方“只看关注”复选框，列表中将展示被设为关注的威胁事件。
- **威胁透视镜**：以图标和箭头连接线的形式展示指定时间周期内所选风险终端发生的威胁事件的关系。箭头连接线代表有威胁产生，箭头的方向表示威胁的方向。
    - 点击上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的威胁事件信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。

弱点

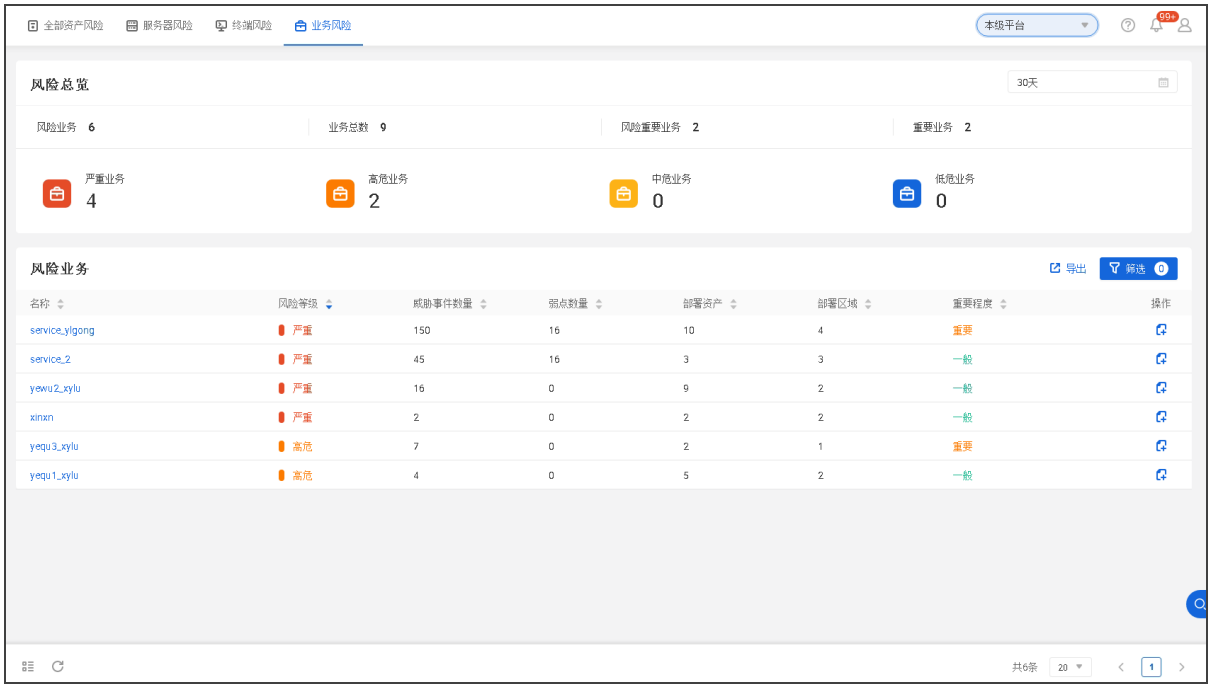


- 上方概览展示所选风险终端存在的弱点总数、各级别弱点的数量。
    - 点击弱点数量对应的数字，系统将全部的弱点显示在页面下方的弱点列表中。
    - 点击各弱点等级对应的数字，系统将根据弱点等级作为筛选条件筛选对应的弱点，显示在页面下方的弱点列表中。
- **弱点类型TOP5**：以柱状图形式展示所选风险终端存在的数量排名前5的弱点类型。
    - 鼠标悬停在柱状图上，显示对应类型弱点的数量。
- **弱点趋势图**：以曲线图的方式展示所选风险终端指定时间内弱点数量的变化趋势。
    - 鼠标悬停在曲线图指定位置上，显示对应时间点弱点的数量。
- 下方列表展示所选风险终端存在的所有弱点列表。
    - 点击上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的弱点信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
    - 点击弱点列表中弱点条目后的按钮，或者在弱点详情页面点击“新建工单”按钮，配置对应的工单对弱点进行响应。

- 点击弱点名称链接，打开所选弱点的详情页面，查看该弱点详细信息、简介、处置建议、参考网站以及受影响的主机列表。

业务风险

点击“风险管理 > 业务风险”，打开业务风险页面，展示业务的安全风险状态总览以及所有风险业务详情列表。



风险状态总览

最上方展示业务的数量统计，包括受到威胁的业务（即风险业务）个数、业务总数、风险重要业务个数以及重要业务个数。

- 仅当设备作为上级平台时，可以选择查看本级平台或指定的下级平台的风险业务信息。点击右上角 本级平台 下拉框，选择查看的平台，下方列表中将展示指定平台的风险业务信息。当选择下级平台时，支持查看和导出风险业务信息，不支持新建工单操作等操作。
- 选择风险发生的时间范围，符合条件的风险业务信息将展示在列表中。默认的时间范围为7天。
  - 点击时间选择下拉框选择“1小时/12小时/24小时/7天/30天”。
  - 自定义“开始时间”和“结束时间”，时间可以精确到秒。“开始时间”可指定为前180天内，且起止时间跨度不能超过30天。
- 点击“风险业务”的数字，刷新下方“风险业务”列表，查看风险业务列表详细信息。

- 点击“业务总数”的数字跳转至"业务管理" 在第369页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"业务管理" 在第369页页面，查看业务列表详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击“风险重要业务”的数字，在下方“风险业务 ”列表查看资产价值为“重要”的风险业务详细信息。
- 点击“重要业务”的数字跳转至"业务管理" 在第369页页面，或者点击“Ctrl+鼠标左键”在新标签页中打开"业务管理" 在第369页页面，查看资产价值为“重要”的业务列表详细信息。若查看的是下级平台的数据，则不支持跳转。
- 点击各级别业务对应的数字，在下方“风险业务 ”列表查看不同风险等级的风险业务详细信息。

风险业务

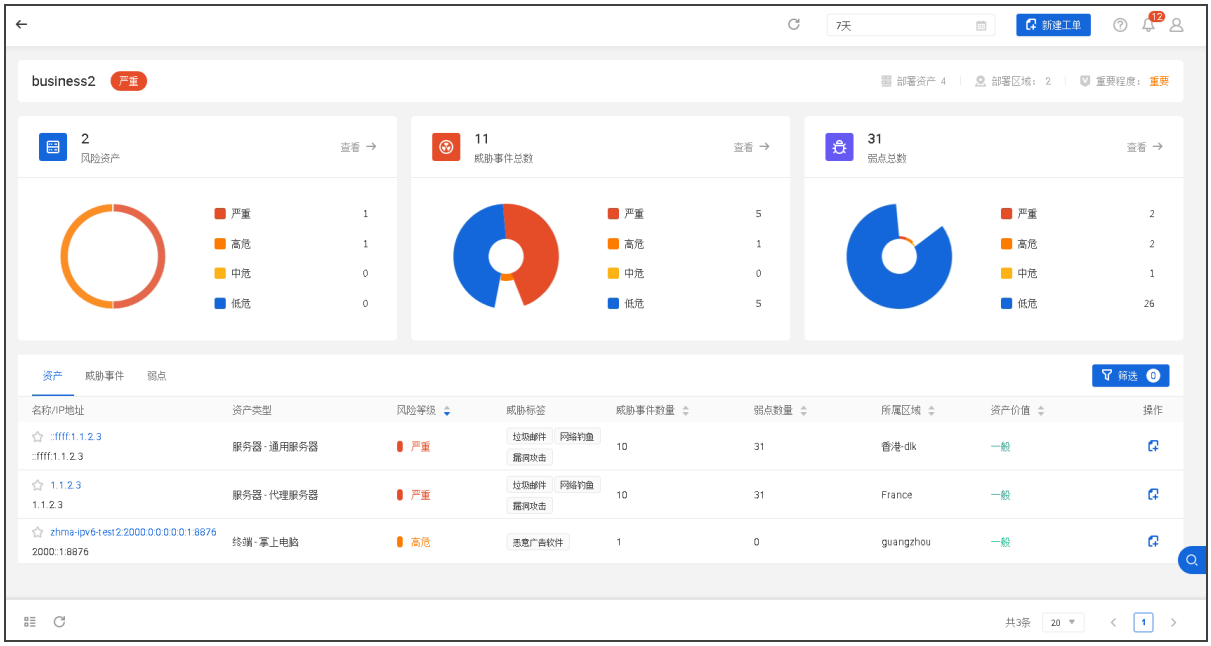
页面下方展示风险业务列表。

- 点击“导出”按钮，以CSV格式导出系统存储的前10000个风险业务信息或者筛选、排序后的前10000个风险业务信息。
- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的风险业务。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。切换平台时自动重置筛选条件。
- 点击列表中风险业务条目后的按钮，或者在风险业务详情页面点击“新建工单”按钮，配置对应的工单对风险业务进行响应。
- 点击业务名称链接，打开所选风险业务的详情页面，查看风险业务详情。
- 点击页面左下角  按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角  按钮，刷新风险业务列表。

查看风险业务详情

在风险业务详细信息页面，从资产、威胁事件、弱点三方面查看所选风险终端详细信息。



- **风险资产**：圆环图展示运行该业务的各风险等级的风险资产的分布统计结果。圆环图中间表示风险资产占比，右侧展示各风险等级的风险资产数量。
    - 点击右侧各风险等级图例或对应的数字，图例变灰色，取消所选风险等级在圆环图的统计展示。
    - 鼠标悬停在圆环图各部分，显示对应风险等级的风险资产数量。
    - 点击圆环图的各部分，在页面下方的资产标签页查看对应风险等级的风险资产详细信息。
    - 点击“查看”，页面下方的资产标签页显示全部风险等级的风险资产详细信息。
- **威胁事件总数**：圆环图展示所选风险业务上发现的未解决威胁事件的分布统计结果，右侧展示各级别的威胁事件数量。
    - 点击右侧各级别图例或对应的数字，图例变灰色，取消所选级别在圆环图的统计展示。
    - 鼠标悬停在圆环图各部分，显示对应级别的威胁事件数量。
    - 点击圆环图的各部分，在页面下方的威胁事件标签页查看对应级别的威胁事件列表详细信息。
    - 点击“查看”，页面下方的威胁事件标签页显示全部级别的威胁事件列表详细信息。

- **弱点总数**：圆环图展示所选风险业务上发现的弱点的分布统计结果，右侧展示各弱点等级的弱点数量。
    - 点击右侧各弱点等级图例或对应的数字，图例变灰色，取消所选弱点等级在圆环图的统计展示。
    - 鼠标悬停在圆环图各部分，显示对应弱点等级的弱点数量。
    - 点击圆环图的各部分，在页面下方的弱点标签页查看对应弱点等级的弱点列表详细信息。
    - 点击“查看”，页面下方的弱点标签页显示全部弱点等级的弱点列表详细信息。
- **资产**：展示运行该业务的风险资产列表。
    - 点击列表中具体资产前的 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- **威胁事件**：展示所选风险业务上发现的威胁事件列表。
- **弱点**：展示所选风险业务上发现的弱点列表。

第6章 事件响应

智源平台可以采集多种类型的数据信息，并通过威胁引擎/攻击链引擎检测威胁事件，将分散部署的各种网络安全设备的威胁事件进行汇总、统计以及分析。针对智源平台中所有威胁事件，系统提供了事件联动响应功能，作为一站式的威胁情报查询和网络安全处置的工具，与网络安全设备、主机安全设备和威胁情报平台进行联动，使用手动响应或自动响应的方式，在智源平台中快速跳转或下发响应配置至联动实体，实现对威胁事件的快速响应处理。同时，还可以配置工单，与威胁事件的联动响应相结合，更直观地对威胁事件的处理过程进行跟踪记录。

事件联动响应方式包含以下两种方式：

- 手动响应：用户在对需要处理的威胁事件进行人工分析后，在智源平台中通过手动方式跳转至联动的安全设备，然后在联动安全设备中配置对威胁事件的响应处理动作，或者在智源平台中对联动的实体安全设备直接配置要下发的策略或IP阻断，进而实现对威胁事件进行响应处理。关于联动实体的配置，请参阅"联动实体" 在第255页。
- 自动响应：系统根据用户已配置的威胁事件响应剧本监测智源平台中的威胁事件，当满足剧本触发条件的威胁事件发生时，将会执行对应的剧本，并按照剧本流程中的后续配置自动完成对威胁事件的响应处理或人工确认是否完成后续对威胁事件的响应处理。关于剧本的介绍，请参阅"剧本管理" 在第216页。

事件响应部分包含如下内容：

- "剧本管理" 在第216页：介绍了如何创建并编排剧本、查看剧本详情、查看剧本响应记录等。
- "联动实体" 在第255页：介绍了如何添加联动实体（网络安全设备、主机安全设备和威胁情报库）、查询威胁情报、配置下发的执行动作。
- "工单管理" 在第281页：介绍了针对威胁事件的处理工单总览、工单列表以及如何新建工单等。

剧本管理

剧本是事件响应的基础，对威胁事件执行响应动作的依据。剧本是指对不同场景下的威胁事件，以流程拓扑图形式编排的特定响应流程。

剧本中包含了针对威胁事件的触发条件、对威胁情报的查询、执行响应的判定条件，以及响应处理动作（网络安全设备动作、主机安全设备动作或者平台动作）。当满足剧本触发条件的威胁事件发

生时，将会执行对应的剧本，按照剧本流程中的后续配置自动完成对威胁事件的响应处理或者进行人工确认是否完成后续对威胁事件的响应处理。

查看剧本

剧本管理页面以数字、圆环图等多种方式展示了各类型剧本和任务的统计概览，以列表形式展示了所有已创建的剧本、待响应任务、中止任务和响应记录的详细信息。点击“事件响应 > 剧本管理”，打开剧本管理页面。



剧本总览

- 在右上角指定时间范围，总览部分和下方列表中将展示指定时间范围内的统计数据。可以选择1小时、12小时、24小时、7天、30天或指定开始时间和结束时间。
- 左侧页面提供了剧本总数，自动化剧本、人工确认剧本、待响应任务、成功任务、失败任务、中止任务的数量。
    - 点击“剧本总数”对应的数字，页面下方<剧本列表>标签页将展示所有剧本。
    - 点击“自动化剧本”或“人工确认剧本”对应的数字，系统将根据剧本类型作为筛选条件，筛选对应的剧本并显示在页面下方<剧本列表>标签页的列表中。
    - 点击“待响应任务”对应的数字，系统将跳转至<待响应任务>标签页，在列表中显示待响应任务。

- 点击“中止任务”对应的数字，系统将跳转至<中止任务>标签页，在列表中显示执行结果为“中止”的任务。
- 点击“成功任务”或“失败任务”对应的数字，系统将跳转至<响应记录>标签页，根据剧本的执行结果作为筛选条件，筛选执行结果为“成功”或“失败”的剧本并在列表中显示。

- 右侧圆环图直观展示了不同状态任务的分布占比情况，图例展示了各个状态任务的具体占比数值。
  - 点击图例或对应的数字，图例变灰，取消所选任务在圆环图中的统计展示。
  - 鼠标悬停在圆环图各部分，显示对应任务的占比数值。
  - 点击圆环图指定部分，在圆环图中突出显示该状态的任务。

查看剧本列表

剧本列表展示了系统中所有的剧本的详细信息，同时用户可以通过配置筛选条件筛选出需要的剧本，方便进行统一查看和管理。

选择“事件响应 > 剧本管理”，选择<剧本列表>标签页，查看已有剧本的详细信息。



- <剧本列表>标签页展示了剧本名称和下发时间、创建人、依赖的联动实体、依赖动作、待响应任务个数、响应次数、剧本配置的校验结果、状态、是否需要人工确认、生效状态、生效时间和操

作等内容。

- 点击上方 

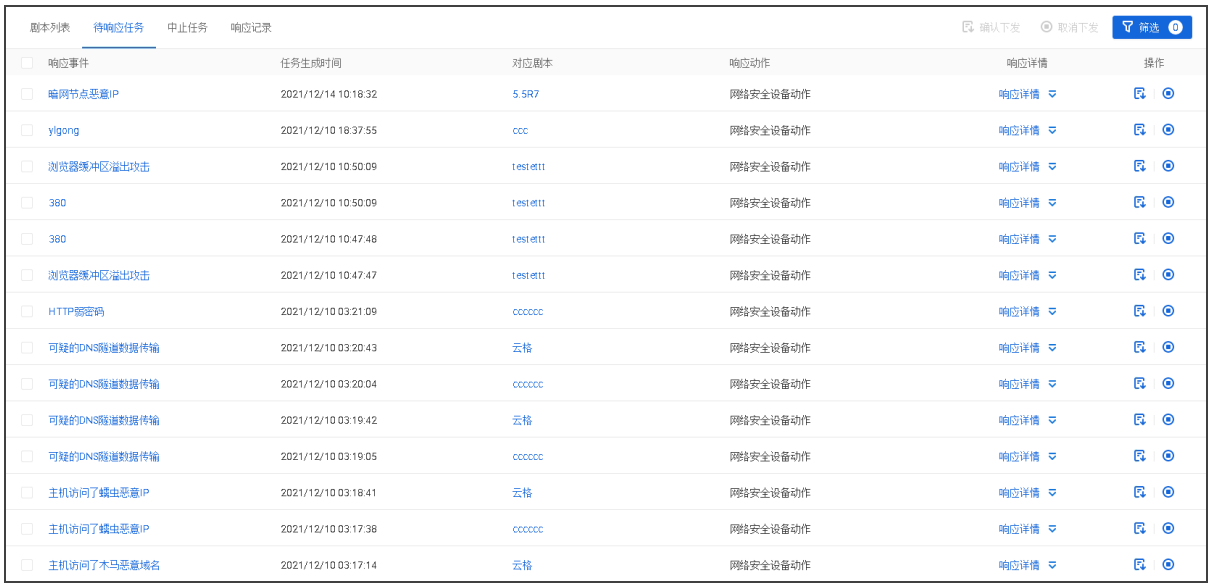
按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的剧本。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 在剧本总览部分选择时间范围后，系统通过筛选剧本的下发时间，在剧本列表展示符合条件的剧本。指定时间范围后，

按钮上数字加一，点击“重置”后，列表中重新展示所有剧本，但不影响总览部分和其他标签页的统计展示。
- 点击“新剧本”按钮，创建新的剧本。
- 勾选剧本复选框，点击“启用”或“禁用”按钮，启用/禁用指定的剧本。
- 点击列表中剧本名称，打开剧本详情页面，查看剧本的详细信息。
- 点击指定剧本“待响应任务”列中的数字，跳转到<待响应任务>标签页，查看该触发剧本的待响应任务。
  - 点击指定剧本“响应次数”列中的数字，打开响应记录页面，查看该剧本的执行历史记录。
- 点击“状态”列的按钮，启用或禁用指定剧本。表示剧本状态为已启用，表示剧本状态为禁用。
- 点击“人工确认”列的按钮，启用或禁用人工确认。表示剧本需要人工确认，表示剧本为自动化剧本。
- 点击列表中指定剧本的按钮，修改所选剧本的基础信息和触发逻辑。
- 点击列表中指定剧本的按钮，删除所选剧本。如需批量删除剧本，勾选多个剧本，点击右上角的“删除”按钮。
- 点击页面左下角按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角按钮，刷新剧本列表。

查看待响应任务

待响应任务列表用于展示匹配了人工确认类型的剧本，且该剧本存在人工确认类型动作的任务。通过响应详情可以查看需要人工确认的动作信息，支持对待响应任务进行批量确认/取消下发。

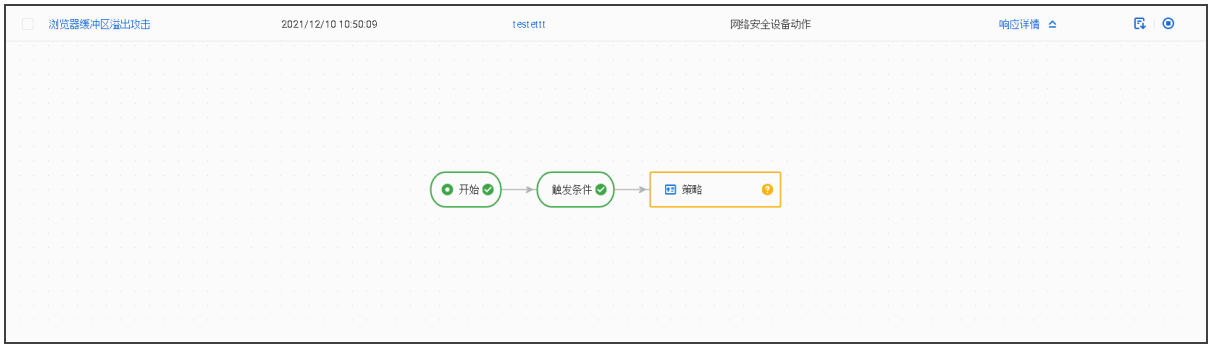
选择“事件响应 > 剧本管理”，选择<待响应任务>标签页，查看所有需要人工确认的任务。



- <待响应任务>标签页展示了威胁事件的名称、任务的生成时间、对应剧本名称、响应动作、响应详情和操作等。
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的待响应任务。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。

- 在剧本总览部分选择时间范围后，系统通过筛选待响应任务的生成时间，在待响应任务列表展示符合条件的任务。指定时间范围后， 筛选 0 按钮上数字加一，点击“重置”后，列表中重新展示所有待响应任务，但不影响总览部分和其他标签页的统计展示。
  - 点击“响应事件”列的事件名称，打开威胁事件，查看该威胁事件的详细信息。
  - 点击“对应剧本”列的剧本名称，查看对应剧本的详细信息。
- 点击“响应详情”展开对应剧本拓扑图，查看该任务在剧本中执行的详细情况。绿色节点表示执行成功的节点。黄色节点表示需要人工确认的节点（当前动作需要人工确认之后才会继续执

行）。



- 点击节点，在打开页面中查看当前节点的执行结果、提示消息、运行数据以及详细配置信息。



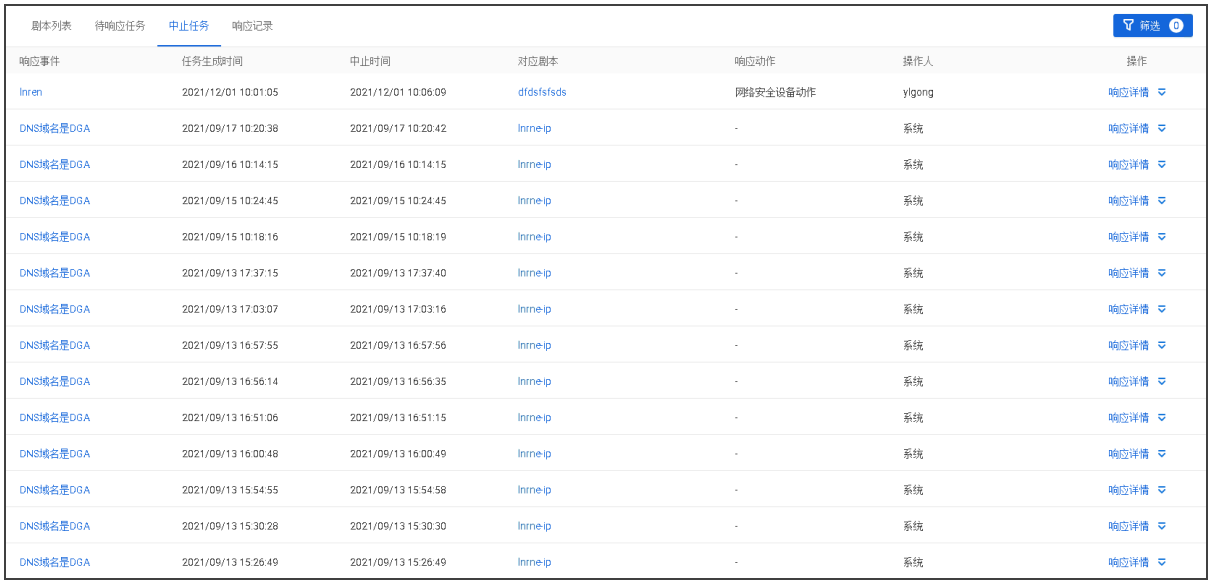
- 点击“操作”列的 按钮，确认下发该待响应任务，该任务将继续执行。点击 按钮，取消下发该待响应任务，该任务被人为中止并添加到中止任务列表。勾选多个待响应任务，点击右上角的“确认下发/取消下发”进行批量操作。

也可以在<剧本列表>标签页，点击“待响应任务”列中的数字，打开待响应任务列表，查看触发了指定剧本的待响应任务。

查看中止任务

中止任务列表用于展示不满足判定条件而被管理员或系统中止的任务。

选择“事件响应 > 剧本管理”，选择<中止任务>标签页，查看所有处于中止状态的任务。



响应事件	任务生成时间	中止时间	对应剧本	响应动作	操作人	操作
lnren	2021/12/01 10:01:05	2021/12/01 10:06:09	dfdsfsfsds	网络安全设备动作	ylgong	响应详情
DNS域名是DGA	2021/09/17 10:20:38	2021/09/17 10:20:42	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/16 10:14:15	2021/09/16 10:14:15	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/15 10:24:45	2021/09/15 10:24:45	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/15 10:18:16	2021/09/15 10:18:19	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 17:37:15	2021/09/13 17:37:40	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 17:03:07	2021/09/13 17:03:16	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 16:57:55	2021/09/13 16:57:56	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 16:56:14	2021/09/13 16:56:35	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 16:51:06	2021/09/13 16:51:15	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 16:00:48	2021/09/13 16:00:49	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 15:54:55	2021/09/13 15:54:58	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 15:30:28	2021/09/13 15:30:30	lnrne-ip	-	系统	响应详情
DNS域名是DGA	2021/09/13 15:26:49	2021/09/13 15:26:49	lnrne-ip	-	系统	响应详情

- <中止任务>标签页展示了威胁事件的名称、任务的生成时间、中止时间、对应剧本名称、响应动作、操作人和操作等。
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的中止任务。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 剧本总览部分选择时间范围后，系统通过筛选中止任务的生成时间，在中止任务列表展示符合条件的任务。指定时间范围后，筛选 0 按钮上数字加一，点击“重置”后，列表中重新展示所有中止任务，但不影响总览部分和其他标签页的统计展示。
- 点击“响应事件”列的事件名称，打开威胁事件，查看该威胁事件的详细信息。
- 点击“对应剧本”列的剧本名称，查看对应剧本的详细信息。
- 点击“操作”列的响应详情展开对应剧本拓扑图，查看剧本执行的详细情况。绿色节点表示执行成功的节点。橙色节点表示执行中止的节点（被人工中止或不满足判定条件被系统中止）。



- 点击节点，在打开页面中查看当前节点的执行结果、提示消息、运行数据以及详细配置信息。



查看剧本响应记录

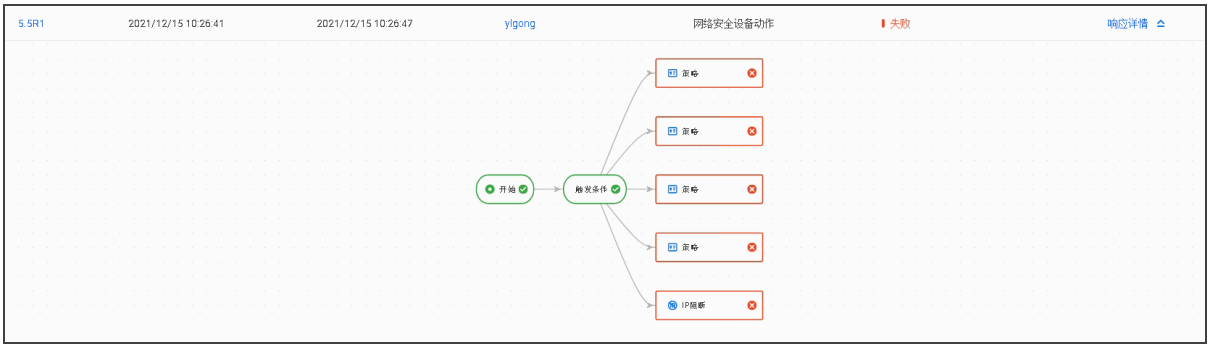
剧本响应记录用于统计剧本中各个动作的调用历史和动作执行结果，用户可以通过剧本响应记录查看剧本的执行情况。

选择“事件响应 > 剧本管理”，选择<响应记录>标签页，查看所有剧本的执行结果。



剧本名称	开始时间	结束时间	响应事件	响应动作	状态	操作
5.5R7	2021/12/21 14:16:59	2021/12/21 14:17:18	恶意软件导致HTTP请求包含不正常的...	网络安全设备动作	成功	响应详情
cccccc	2021/12/21 14:16:59	2021/12/21 14:17:04	恶意软件导致HTTP请求包含不正常的...	网络安全设备动作	成功	响应详情
5.5R7	2021/12/21 09:32:11	2021/12/21 09:32:46	ylgong	网络安全设备动作	成功	响应详情
cccccc	2021/12/21 09:32:11	2021/12/21 09:32:27	ylgong	网络安全设备动作	成功	响应详情
5.5R7	2021/12/20 17:45:00	2021/12/20 17:45:50	发起主机地址扫描攻击	网络安全设备动作	成功	响应详情
5.5R7	2021/12/20 17:45:00	2021/12/20 17:45:44	发起主机端口扫描攻击	网络安全设备动作	成功	响应详情
5.5R7	2021/12/20 17:45:00	2021/12/20 17:45:44	遭受SYN端口扫描攻击	网络安全设备动作	成功	响应详情
5.5R7	2021/12/20 17:45:00	2021/12/20 17:45:38	遭受端口扫描攻击	网络安全设备动作	成功	响应详情
5.5R7	2021/12/20 17:45:00	2021/12/20 17:45:38	发起SYN端口扫描攻击	网络安全设备动作	成功	响应详情
cccccc	2021/12/20 17:45:00	2021/12/20 17:45:05	遭受SYN端口扫描攻击	网络安全设备动作	成功	响应详情
cccccc	2021/12/20 17:45:00	2021/12/20 17:45:05	发起主机地址扫描攻击	网络安全设备动作	成功	响应详情
cccccc	2021/12/20 17:45:00	2021/12/20 17:45:05	遭受端口扫描攻击	网络安全设备动作	成功	响应详情
cccccc	2021/12/20 17:45:00	2021/12/20 17:45:05	发起SYN端口扫描攻击	网络安全设备动作	成功	响应详情
cccccc	2021/12/20 17:45:00	2021/12/20 17:45:05	发起主机端口扫描攻击	网络安全设备动作	成功	响应详情

- <响应记录>标签页展示了剧本的名称、执行开始时间、结束时间、执行响应的威胁事件、响应执行的成功/失败/中止状态以及操作等。
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的剧本响应记录。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 剧本总览部分选择时间范围后，系统通过筛选剧本执行的开始时间，在响应记录列表展示符合条件的响应。指定时间范围后，筛选 0 按钮上数字加一，点击“重置”后，列表中重新展示所有响应，但不影响总览部分和其他标签页的统计展示。
- 点击“剧本名称”列的剧本名称，查看对应剧本的详细信息。
  - 点击“响应事件”列的事件名称，打开威胁事件，查看该威胁事件的详细信息。
  - 点击“操作”列的响应详情展开对应剧本拓扑图，查看剧本执行的详细情况。绿色节点表示执行成功的节点。橙色节点表示执行中止的节点（被人工中止或不满足判定条件被系统中止）。红色节点表示执行失败的节点。



- 点击节点，在打开页面中查看当前节点的执行结果、提示消息、运行数据以及详细配置信息。



也可以在<剧本列表>页面，点击“响应次数”列中的数字，打开指定剧本的所有响应记录页面。



查看剧本详情

剧本详情包括剧本的基础信息和触发逻辑。

选择“事件响应 > 剧本管理”，选择<剧本列表>标签页，点击列表中指定剧本名称，点击<基础信息>标签页，打开剧本基础信息页面。

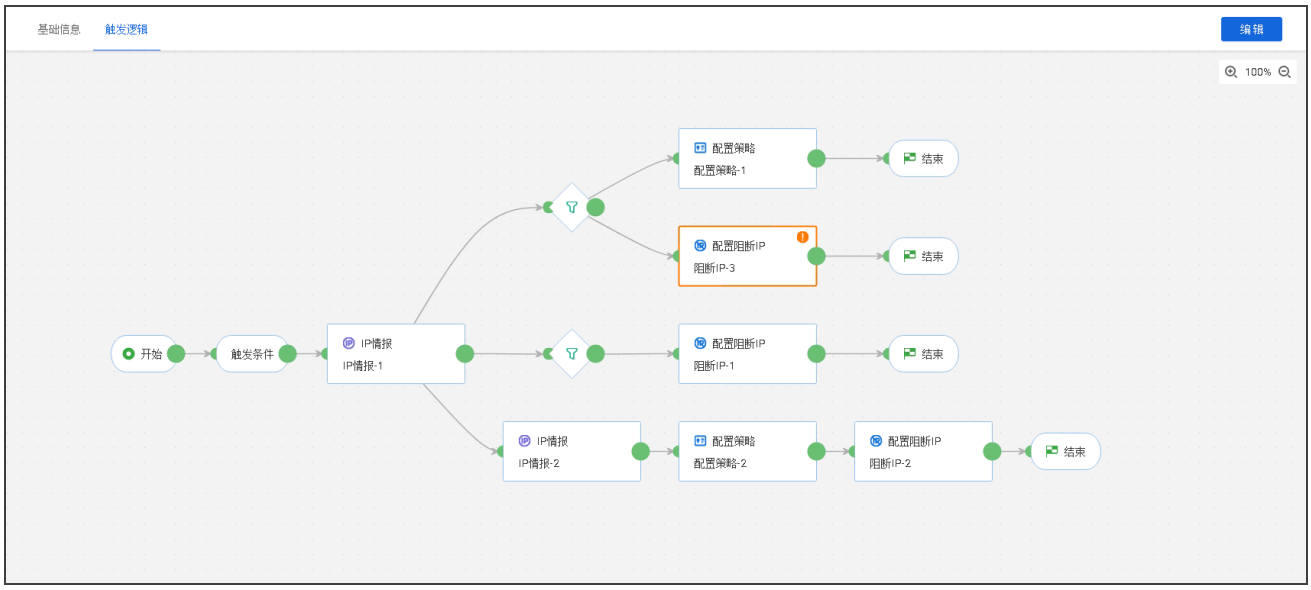


- 页面展示了该剧本的名称、生效时间、剧本类型和剧本描述。剧本会在指定的生效时间内生效，若没有配置生效时间，则该剧本永久有效。系统支持2种剧本类型，分别为“自动化剧本”和“人工确认剧本”。配置为自动化剧本后，在满足触发条件时会自动下发任务；配置为人工确认剧本后，可以选择启用邮件通知功能，当剧本被触发时，会发送邮件给对应联系人通

知其进行人工确认。

- 点击“编辑”按钮，编辑剧本的基础信息。

选择“事件响应>剧本管理”，选择<剧本列表>标签页，点击列表中指定剧本名称，点击<触发逻辑>标签页，打开剧本触发逻辑页面。



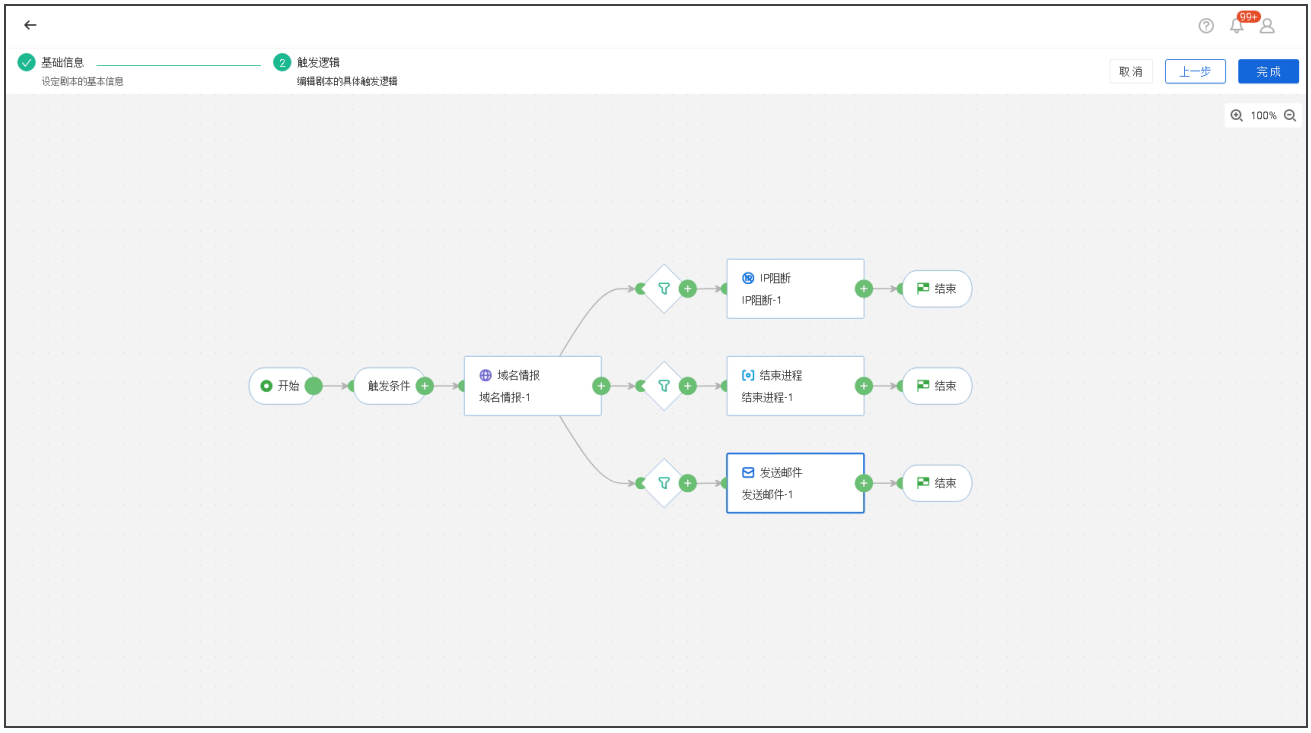
- 带“！”的节点表示该节点的配置无效，提示用户需要检查该节点的配置。
- 点击节点，在打开页面中查看对应的配置信息。
- 点击“编辑”按钮，进入该剧本的编排状态，即可编辑剧本的各节点配置信息。

配置剧本

剧本的完整配置流程建议为：开始→配置剧本的基础信息→配置剧本的触发条件→配置威胁情报库动作→配置判定条件→配置网络安全设备动作/配置主机安全设备动作→配置平台动作→结束。

在剧本管理页面，点击“新剧本”按钮，进行剧本配置。剧本配置包括两个步骤：配置剧本基本信息和配置剧本的触发逻辑。在<基础信息>标签页配置剧本的名称、生效时间、剧本类型以及剧本描述等基础信息。在<触发逻辑>标签页根据剧本的配置流程，完成剧本的完整编排。

下图展示了配置完成的剧本详细内容：



- 下方为剧本对应的拓扑图画板，以流程拓扑图方式展示了剧本的完整流程。
- 点击流程拓扑图节点，对应的编辑窗口将会从左侧弹出，可以查看或编辑配置的内容。
- 鼠标按住剧本的流程拓补图，可以整体移动拓其位置。
- 右上角百分比显示当前拓补图的显示比例，可以点击或按钮放大或缩小拓扑图。
- 点击节点处的按钮，打开<剧本模块>页面，选择节点的类型后点击“确定”按钮，新的节点即可添加完成，同时可以在左侧编辑页面中配置对应的内容。
- 点击节点右上方的×按钮，删除需要删除的节点。删除后，该节点之后相连的所有节点均会被一同删除。

预定义剧本

系统提供5个预定义剧本，可作为剧本编排的模板，其中已经预定义了剧本的逻辑，用户可以参考预定义剧本的样例，通过完善剧本的配置，补充剧本的联动实体和联动动作等相关内容使得剧本完整并生效。

预定义剧本详细介绍如下：

预定义剧本名称	预定义内容说明	需完善内容说明
Web业务系统弱密码自动通报（模板）	在发现Web业务系统存在弱密码时，自动创建工单，告知相关管理人员及时处理，防止由弱密码引起进一步损失。	在此模板上，用户需要补充联动设备相关信息和工单信息。
暴力破解类威胁自动封堵（模板）	在发现暴力破解类威胁时(包含大部分网络协议)，自动阻断攻击者IP地址，并发送邮件通知至相关人员。	在此模板上，用户需要补充IP阻断的详细配置和邮件通知联系人信息。
访问勒索软件恶意域名自动封禁（模板）	在发现主机有访问勒索软件域名行为时，自动联动网络安全设备，封堵该域名对应的IP地址，并发送邮件通知相关人员。	在此模板上，用户需要补充联动设备相关信息，并设置阻断的IP为域名对应的IP，同时补充邮件联系人信息。
挖矿软件自动隔离（模板）	在发现挖矿软件行为时，自动联动主机安全设备对挖矿软件进程进行结束和隔离，发送邮件通知至相关人员。	在此模板上，用户需要补充联动设备相关信息及邮件通知联系人信息。
挖矿通信行为自动阻断（模板）	在发现挖矿通信行为时，自动对域名情报进行二次确认，在确认是挖矿通信行为时，自动阻断通信IP地址，并发送邮件通知至相关人员。	在此模板上，用户需要补充联动设备相关信息及邮件通知联系人信息。



注意:

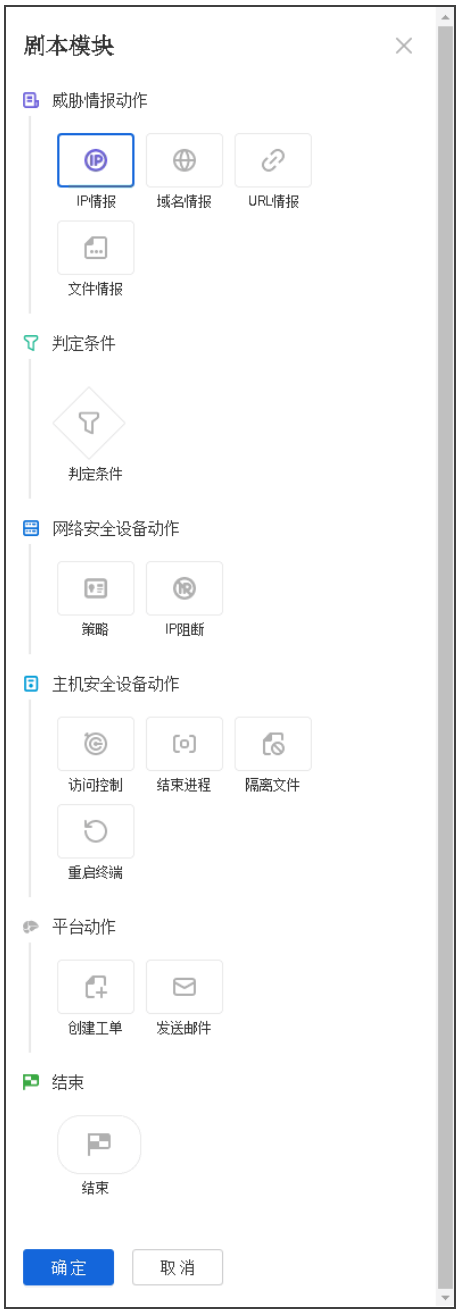
- 预定义剧本支持修改、删除。
- 修改配置后的预定义剧本在保存后，预定义的内容将会被覆盖。

创建剧本

新建剧本并编排剧本内容，请按照以下步骤进行操作：

1. 点击“事件响应 > 剧本管理 ”，打开剧本管理页面。
2. 点击“新剧本”按钮，进行剧本配置。
3. 在<基础信息>标签页，配置剧本的基本信息。
4. 点击“下一步”，进入<触发逻辑>标签页进行剧本编排。系统已默认添加“开始”节点和“触发条件”节点。
5. 在左侧<触发条件>页面配置剧本触发条件。

6. 点击“触发条件”节点处的按钮，打开剧本模块页面，选择节点类型并添加至剧本。



7. 可以根据需求，继续点击节点处的按钮，在<剧本模块>页面中选择并添加后续新节点，完成配置威胁情报库动作、配置判定条件、配置网络安全设备动作、配置主机安全设备动作或者配置平台动作。

8. 完成上述步骤，并且在添加“结束”节点后，即可完成剧本的整体配置。

9. 点击“完成”按钮，返回到剧本列表页面，该剧本即已添加至剧本列表第一行中。

配置剧本基础信息

配置剧本的基础信息，请按照以下步骤进行操作：

1. 点击“事件响应 > 剧本管理 ”，打开剧本管理页面。点击“新剧本”按钮，进入<基础信息>页面。



在<基础信息>页面，配置剧本的基础信息。

选项	说明
剧本名称（必填项）	指定剧本的名称，最多支持配置73个英文字符或24个中文字符。
生效时间	指定剧本的生效时间。剧本在配置的时间内生效，威胁事件只会匹配生效中的剧本。若不配置生效时间，则剧本永久有效。在弹出框内选择剧本生效的开始时间和结束时间，可以只配置开始时间或结束时间，精确到秒。
剧本类型（必填项）	指定剧本的类型，可以选择“自动化剧本”或“人工确认剧本”，默认为自动化剧本。自动化剧本在满足触发条件后会自动下发任务；人工确认剧本在满足触发条件后需要人工确认是否执行配置的动作，人工选择“确认下发”或“取消下发”。

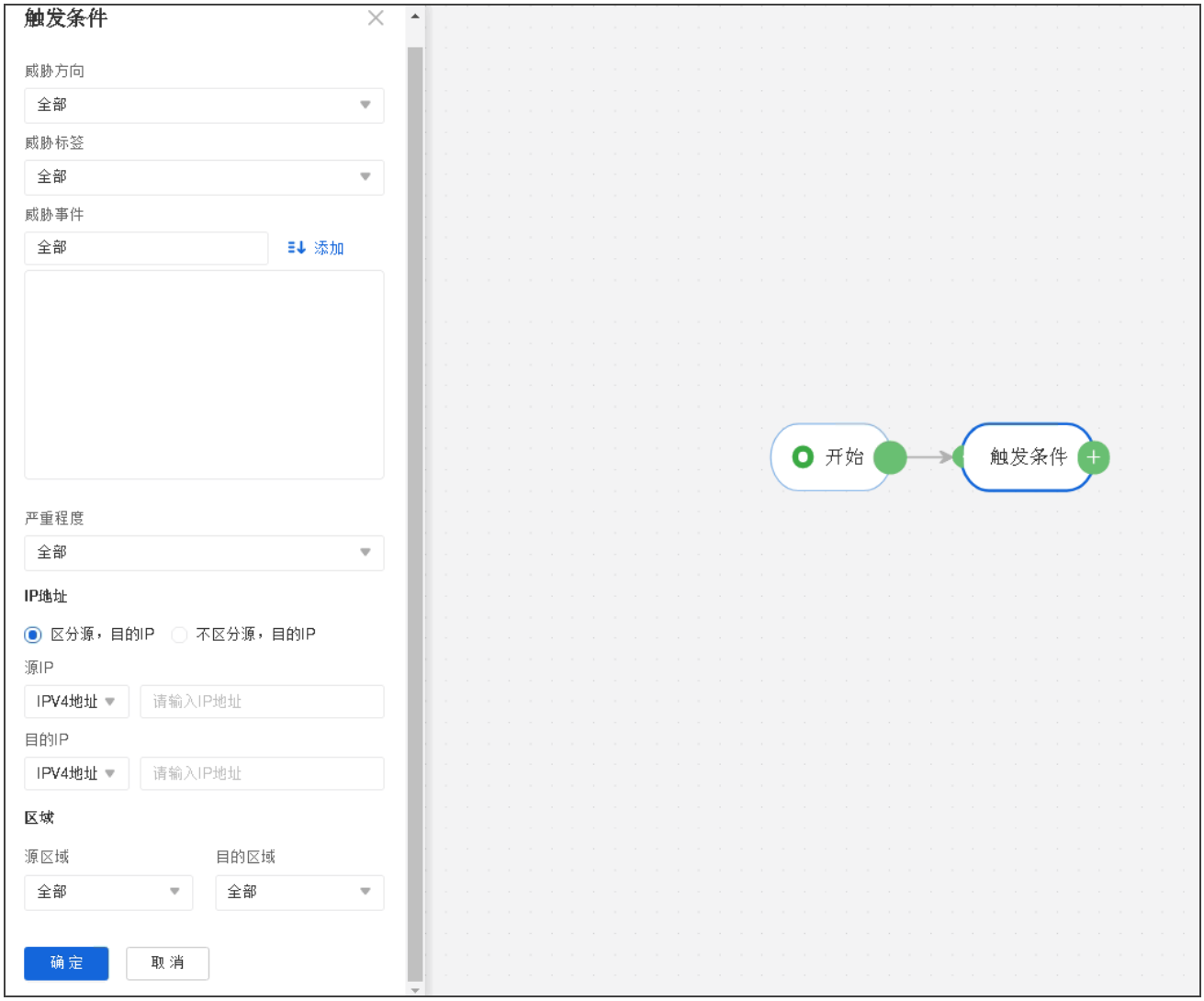
选项	说明
	若指定剧本类型为“人工确认剧本”，可以选择配置邮件通知功能。启用邮件通知功能后，当剧本被触发时，会发送邮件给对应联系人通知其进行人工确认。点击下拉菜单打开联系人列表，选择确认剧本的处理人。 • 在搜索框中输入指定的联系人名称，点击 搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“选择联系人”选项中已选择的联系人。 请先确保已配置好邮件服务器。关于邮件服务器的配置，请参阅"通讯配置" 在第469页。
剧本描述	指定剧本描述。在文本框中输入对剧本的描述，取值范围为0至256个字符。

2. 点击“下一步”，进入<触发逻辑>页面，进行剧本的编排。

配置剧本触发条件

进行剧本编排时，首先需要配置剧本的触发条件，通过触发条件来匹配相应的威胁事件，当满足剧本触发条件的威胁事件发生时，将按照剧本流程中的后续配置对该威胁事件实现自动响应或者进行人工确认是否执行响应动作。

新建剧本后，系统已默认添加“开始”节点和“触发条件”节点，并已打开<触发条件>页面。



在<触发条件>页面，配置触发条件详细信息。

选项	说明
威胁方向	指定剧本匹配的威胁事件的方向。可多选，默认选择全部方向。
威胁标签	指定剧本匹配的威胁事件的标签。可多选，默认选择全部威胁标签。
威胁事件	指定剧本匹配的威胁事件的名称，可以选择当前智源平台中的所有引擎管理中可以报出的威胁事件，也可以手动输入其他威胁事件名称并支持模糊匹配，然后点击“添加”按钮。如不填写则默认选择全部。 **注意**：如指定多个威胁事件，不同威胁事件之间为“或”的关系。
严重程度	指定剧本匹配的威胁事件的严重程度，包括严重、高、中、低，可多选，默认选择全部。

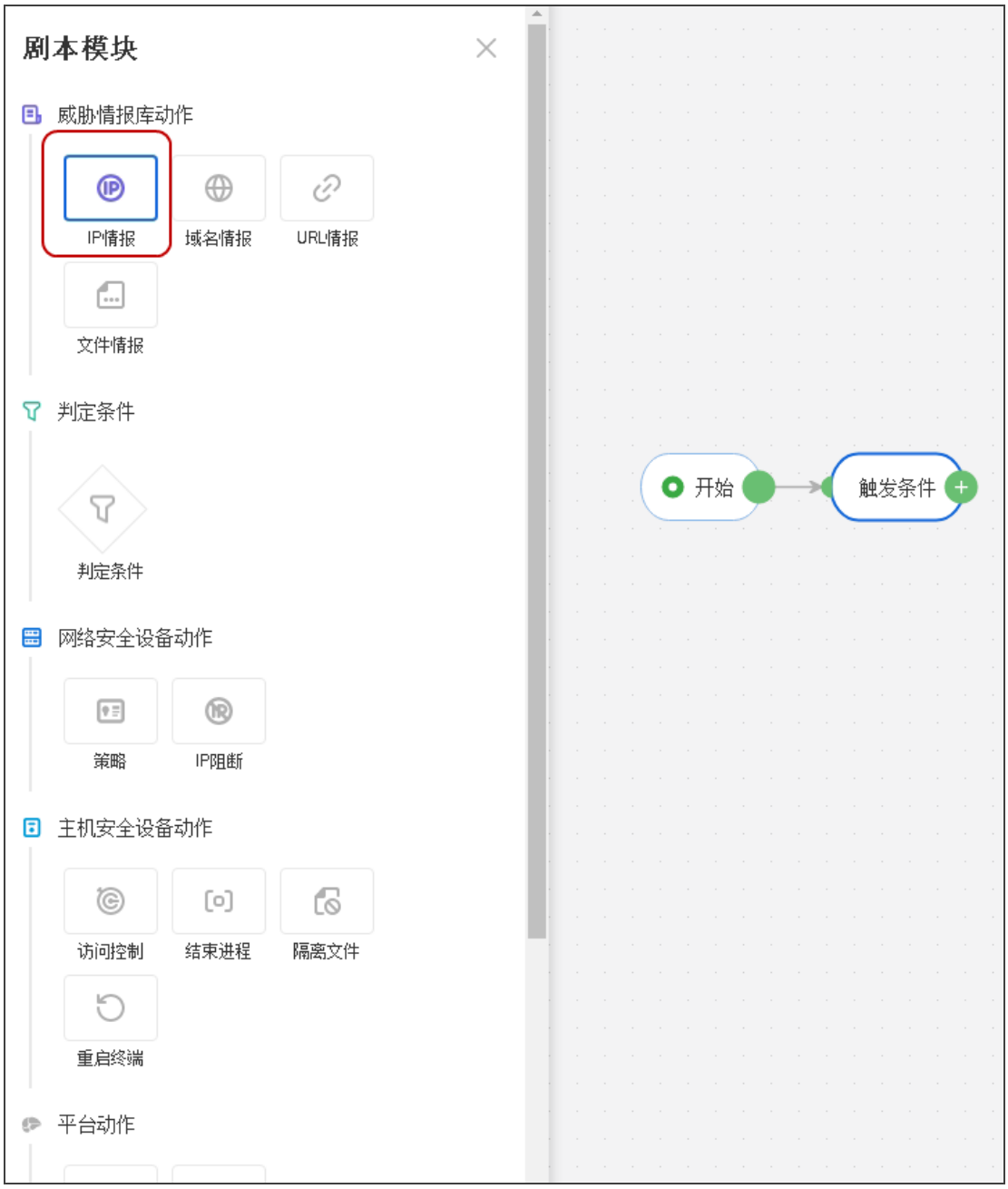
选项	说明
IP地址	
区分源、目的IP	选择区分源、目的IP，在下方配置剧本匹配的威胁事件的源IP、目的IP，可以仅配置源IP或目的IP。当区分源、目的IP时，威胁事件的源、目的IP均须满足配置的源、目的IP，才算匹配成功。指定剧本匹配的威胁事件的源、目的IP，请按照以下步骤操作： 1. 点击“区分源、目的IP”。 2. 点击“源IP”或“目的IP”后的下拉菜单，选择“IPv4地址”、“IPv6地址”、“IPv4地址段”或“IPv6地址段”。 3. 选择“IPv4地址”或“IPv6地址”，在“源IP”或“目的IP”文本框中输入相应类型的IP地址，可以仅配置源IP或目的IP；选择“IPv4地址段”或“IPv6地址段”，在“源IP”或“目的IP”文本框中输入相应类型的起始IP地址和结束IP地址，可以仅配置源IP或目的IP。
不区分源、目的IP	选择不区分源、目的IP，在下方配置剧本匹配的威胁事件的IP地址。当不区分源、目的IP时，威胁事件只需源IP或目的IP匹配配置的IP地址，即匹配成功。指定剧本匹配的威胁事件的IP地址，请按照以下步骤操作： 1. 点击“不区分源、目的IP”。 2. 点击“IP地址”后的下拉菜单，选择“IPv4地址”、“IPv6地址”、“IPv4地址段”或“IPv6地址段”。 3. 选择“IPv4地址”或“IPv6地址”，在“IP地址”文本框中输入相应类型的IP地址；选择“IPv4地址段”或“IPv6地址段”，在“IP地址”文本框中输入相应类型的起始IP地址和结束IP地址。
区域	
源区域	指定剧本匹配的威胁事件的源IP所属的区域。
目的区域	指定剧本匹配的威胁事件的目的IP所属的区域。

配置威胁情报库动作

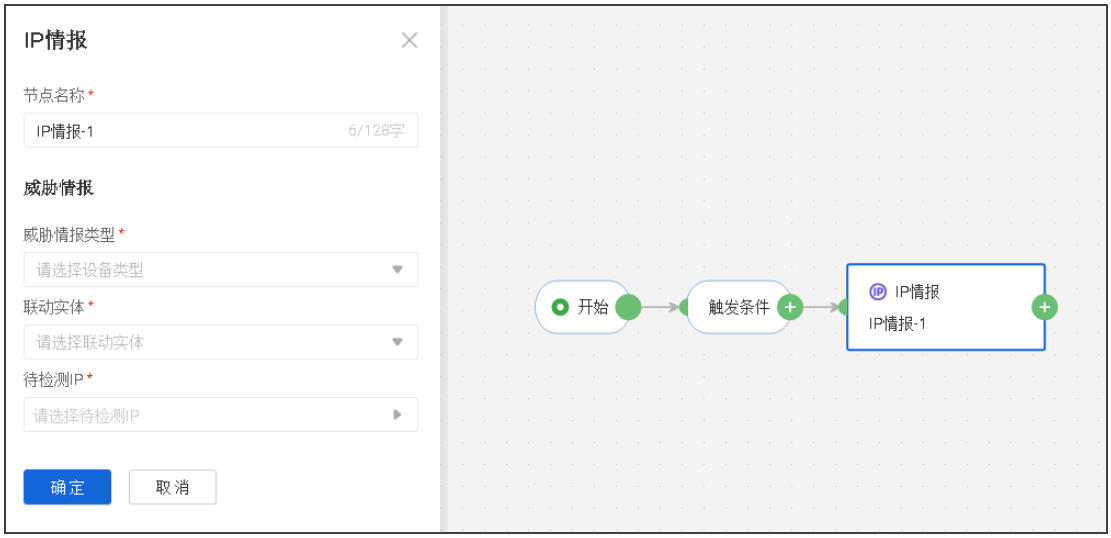
剧本中支持配置的威胁情报库动作为：IP情报、域名情报、URL情报、文件情报。

添加威胁情报库动作（以添加IP情报节点为例），请按照以下步骤进行操作：

1. 点击 按钮，在<剧本模块>页面，点击需要添加的威胁情报库动作，例如：点击“IP情报”。



2. 点击“确定”按钮，“IP情报”节点即添加至剧本拓扑图中。同时，左侧打开<IP情报>页面。



在<IP情报>页面，配置IP情报动作详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。
威胁情报类型（必填项）	选择威胁情报库的设备类型，目前仅支持选择“云瞻”和“VirusTotal”。
联动实体（必填项）	选择该威胁情报库动作需要关联的联动实体，点击下拉菜单选择已添加的威胁情报库实体。关于添加威胁情报库实体，请参阅添加威胁情报库实体。
待检测IP（必填项）	指定进行IP情报查询的IP地址。 点击下拉菜单，在打开的<待检测IP>页面，选择待检测的IP地址类型。例如，选择事件的源IP，即为对匹配触发条件的威胁事件源IP进行IP情报查询。

3. 点击“确定”完成该节点的配置。

配置判定条件

判定条件是指执行后续响应处理动作的判断条件。

配置判定条件，请按照以下步骤进行操作：

1. 点击按钮，打开<剧本模块>页面。

2. 点击“判定条件”。



3. 点击“确定”按钮，“判定条件”节点即添加至剧本拓扑图中。同时，左侧打开<判定条件>页面。



在<判定条件>页面，配置判定条件详细信息。

选项	说明
节点名称（必填项）	指定判定条件的名称，范围是1到128个字符。
条件内容（必填项）	选择需要进行判定的条件内容，该内容与触发条件中的威胁事件或之前节点的内容相关联。例如：假如判定条件之前节点为“触发条件”和“IP情报”，那么判定条件的可选内容即为“事件”或“IP情报”。 1. 点击“条件内容”下拉菜单，在打开的<条件>页面中选择判定条件的内容，点击“确定”按钮。 2. 在条件内容下方文本框/下拉菜单中指定判定值。 3. 点击 按钮，可以添加多个判定条件。 4. 点击“或”/“且”下拉菜单，指定多个判定条件之间的关系。仅可以指定为一种关系，即全为“或”的关系或者全为“且”。

选项	说明
	如上图中样例所示：判定条件是当符合剧本触发条件的威胁事件名称为DGA或者IP情报查询的信誉度为恶意时，将会执行后续的自动响应动作或进行人工确认是否执行响应动作。

4. 点击“确定”完成该节点的配置。

配置网络安全设备动作

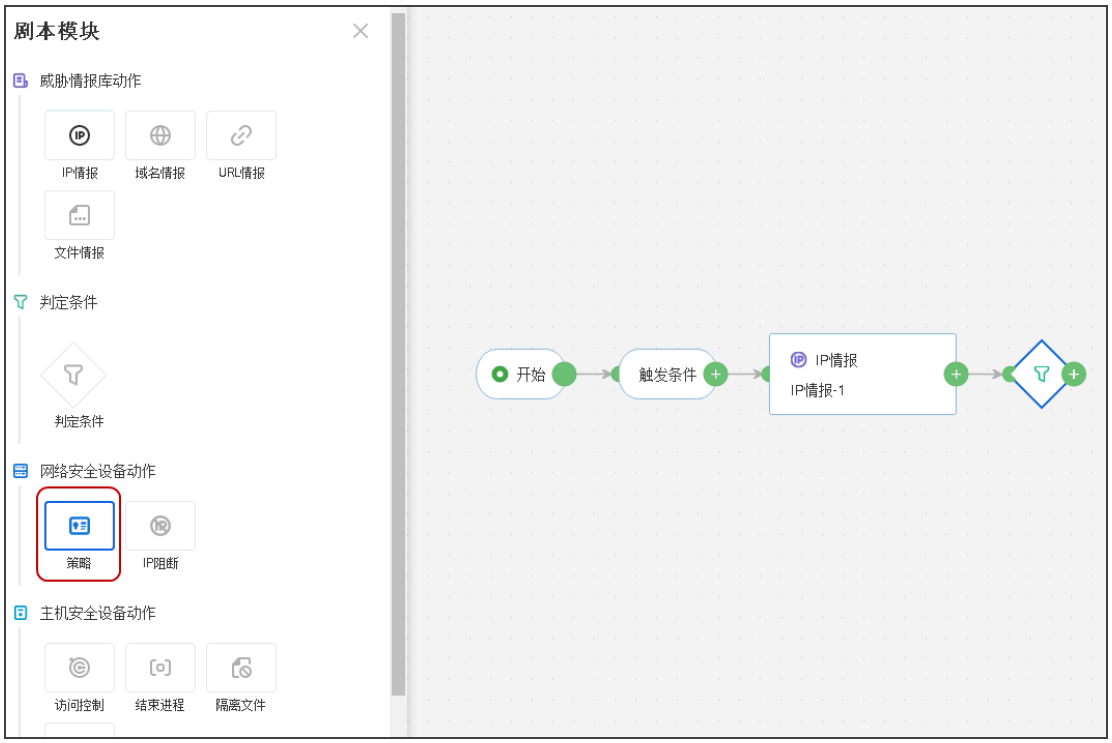
在剧本的编排中，需要指定网络安全设备对威胁事件执行的响应处理动作。自动化剧本将自动执行该响应处理动作，人工确认剧本需要人工确认是否执行该响应处理动作。

剧本中支持配置的网络安全设备动作有：配置策略、配置IP阻断。

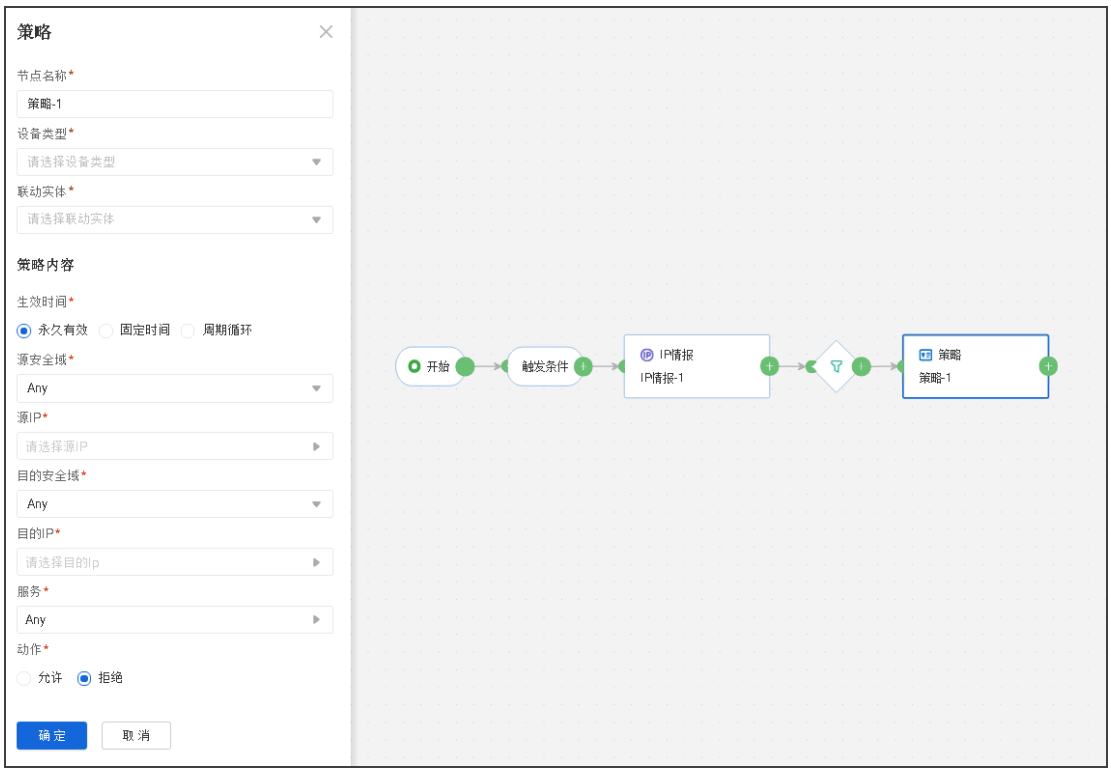
配置策略

配置策略规则，请按照以下步骤进行操作：

1. 点击按钮，在<剧本模块>页面，点击网络安全设备动作“策略”。



2. 点击“确定”按钮，“策略”节点即添加至剧本拓扑图中。同时，左侧打开<策略>页面。



在<策略>页面，配置策略规则详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，最多支持配置95个英文字符或31个中文字符。
设备类型（必填项）	选择执行该策略规则的设备类型。
联动实体（必填项）	选择该策略规则需要关联的网络安全设备联动实体，点击下拉菜单选择已添加的网络安全设备实体。关于添加网络安全设备实体，请参阅添加网络安全设备实体。
策略内容	
生效时间（必填项）	指定策略的生效时间，可以选择“永久有效”、“固定时间”或“周期循环”。 • 选择“永久有效”，则该策略一直处于生效状态。

选项	说明
	• 选择“固定时间”，配置策略生效的“开始时间”和“结束时间”，精确到小时，可以只配置“开始时间”或“结束时间”。未到“开始时间”的策略状态为“待生效”；在“开始时间”和“结束时间”内的策略状态为“生效中”；超过“结束时间”的策略状态为“已失效”。 • 选择“周期循环”，选择循环的周期和起止时间，循环周期可选择每周的某一天，可多选。精确到小时。处于“循环周期”内的策略状态为“生效中”；在“循环周期”外的策略状态为“待生效”。
源安全域（必填项）	指定响应策略规则的源安全域。
源IP（必填项）	点击下拉菜单，在打开的<源IP>页面，指定响应策略规则的源地址。例如，选择事件的源IP，即为对匹配触发条件的威胁事件源地址执行该策略规则。“Any”，表示选择任意源地址。
目的安全域（必填项）	指定响应策略规则的源安全域。
目的IP（必填项）	点击下拉菜单，在打开的<目的IP>页面，指定响应策略规则的目的地址。例如，选择事件的目的IP，即为对匹配触发条件的威胁事件目的地址执行该策略规则。“Any”，表示选择任意目的地址。
服务（必填项）	指定响应策略规则的服务。 • 选择“Any”，表示选择任意服务。 • 选择“自定义”，并在下方指定协议类型、服务目的端口号和服务源端口号，指定自定义服务。
执行操作（必填项）	指定对匹配策略规则的流量所采取的行为， 包括允许和拒绝。

3. 点击“确定”完成该节点的配置。

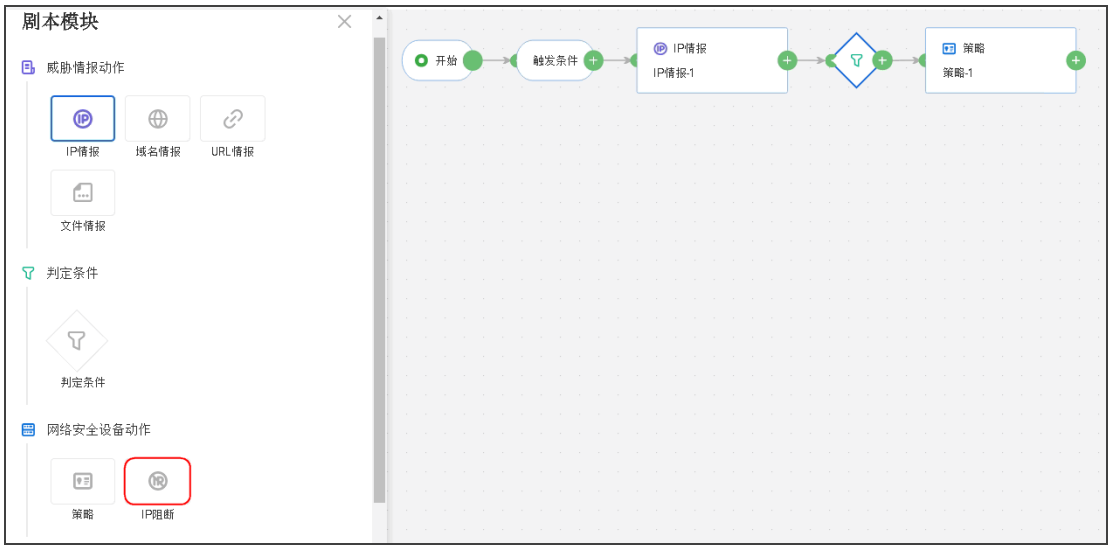


注意: 源IP和目的IP不能同时配置为Any。

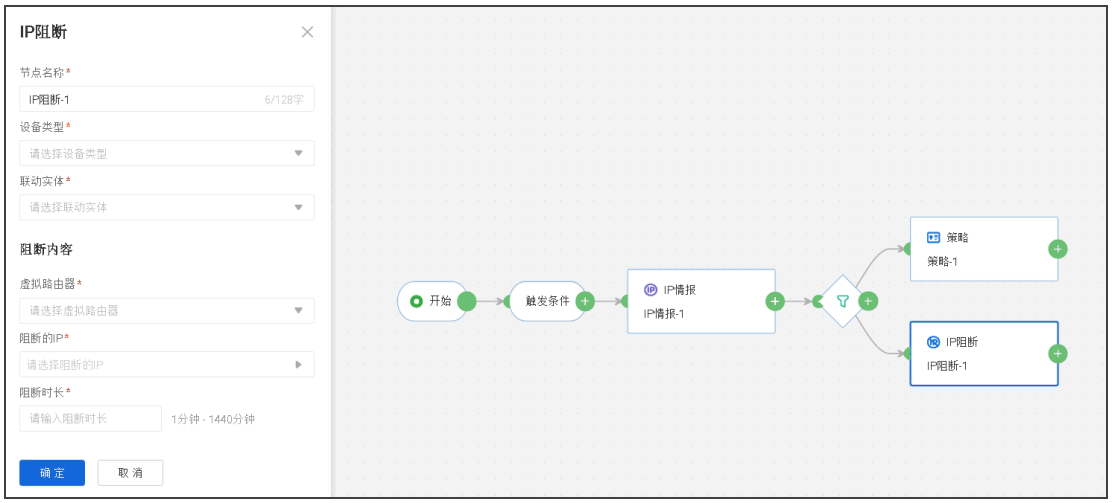
配置IP阻断

配置IP阻断，请按照以下步骤进行操作：

1. 点击按钮，在<剧本模块>页面，点击网络安全设备动作“IP阻断”。



2. 点击“确定”按钮，“阻断IP”节点即添加至剧本拓扑图中。同时，左侧打开<IP阻断>页面。



在<IP阻断>页面，配置IP阻断详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。

选项	说明
设备类型（必填项）	选择执行IP阻断的设备类型。
联动实体（必填项）	选择IP阻断需要关联的联动实体，点击下拉菜单选择已添加的网络安全设备实体。关于添加网络安全设备实体，请参阅添加网络安全设备实体。
阻断内容	
虚拟路由器（必填项）	在下拉菜单中选择被阻断IP所属的虚拟路由器。
阻断的IP（必填项）	点击下拉菜单，在打开的<阻断的IP>页面，指定需要被阻断的IP类型。例如，选择事件的源IP，那么将会对匹配触发条件的威胁事件，执行阻断其源地址。
阻断时长（必填项）	在文本框中输入IP地址将被阻断的时长， 单位为分钟， 范围是1到1440分钟。

3. 点击“确定”完成该节点的配置。

配置主机安全设备动作

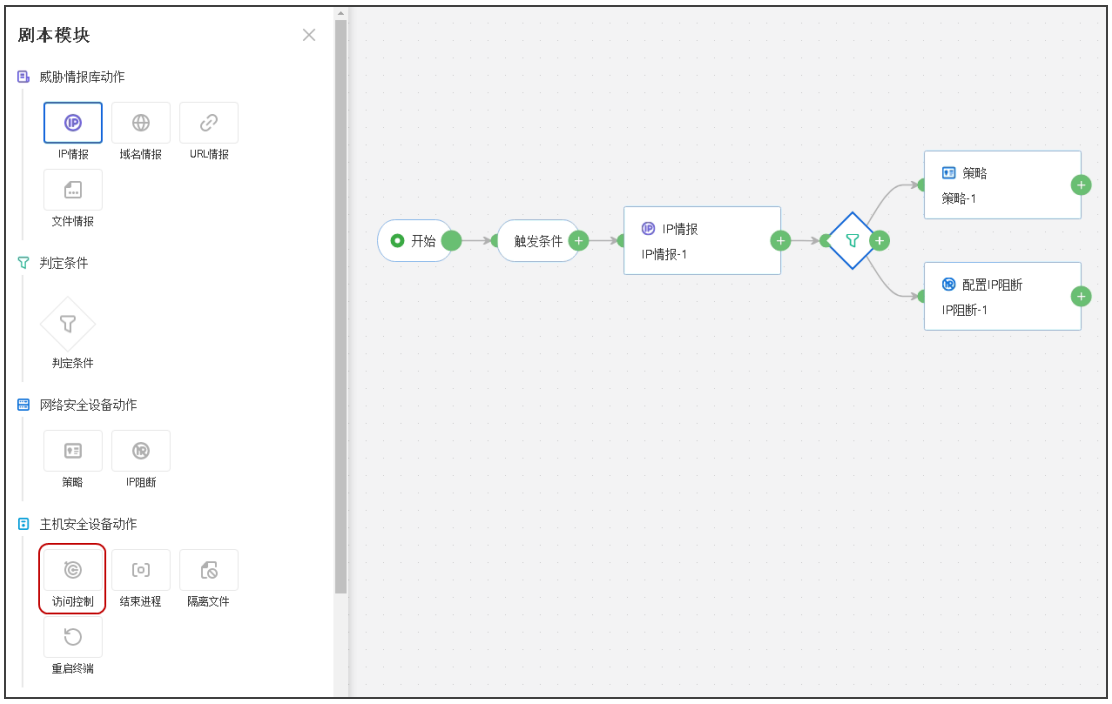
在剧本的编排中，需要指定主机安全设备对威胁事件执行的响应处理动作。自动化剧本将自动执行该响应处理动作，人工确认剧本需要人工确认是否执行该响应处理动作。

剧本中支持配置的主机安全设备响应处理动作有：访问控制、结束进程、隔离文件、重启终端。

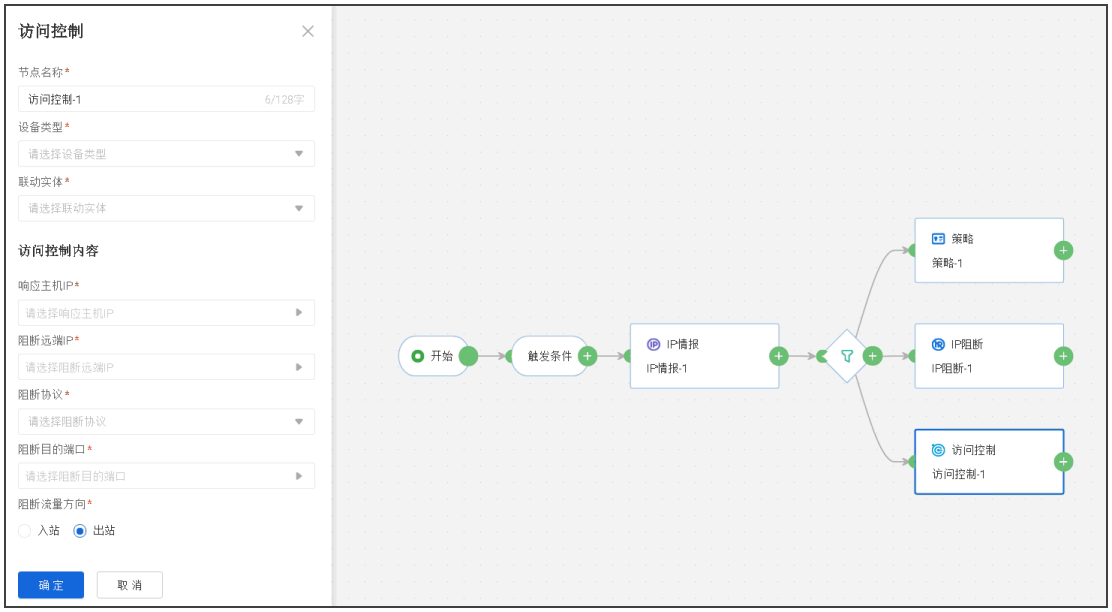
配置访问控制

配置响应的访问控制，请按照以下步骤进行操作：

1. 点击按钮，在<剧本模块>页面，点击主机安全设备动作“访问控制”。



2. 点击“确定”按钮，“访问控制”节点即添加至剧本拓扑图中。同时，左侧打开<访问控制>页面。



在<访问控制>页面，配置访问控制详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。
设备类型（必填项）	选择执行访问控制的设备类型。
联动实体（必填项）	选择访问控制需要关联的联动实体，点击下拉菜单选择已添加的主机安全设备实体。关于添加主机安全设备实体，请参阅添加主机安全设备实体。
访问控制内容	
响应主机IP（必填项）	点击下拉菜单，在打开的<响应主机IP>页面，指定响应的主机IP地址。例如，选择事件的源IP，即将对匹配触发条件的威胁事件源地址指定为响应的主机IP地址。
阻断远端IP（必填项）	点击下拉菜单，在打开的<阻断远端IP>页面，指定需要被阻断的远端IP地址。例如，选择事件的目的IP，即为对匹配触发条件的威胁事件，阻断响应主机IP与该目的地址之间的通信。
阻断协议（必填项）	点击下拉菜单选择需要被阻断的协议类型。
阻断目的端口（必填项）	点击下拉菜单，在打开的<阻断目的端口>页面，指定需要被阻断的目的端口号。例如，选择事件的源端口，即为对匹配触发条件的威胁事件，阻断响应主机IP与该目的端口之间的通信。
阻断流量方向（必填项）	点击“入站”或“出站”单选按钮，指定阻断流量方向。 • 入站：阻断远端IP对响应主机的访问。 • 出站：阻断响应主机对远端IP的访问。

3. 点击“确定”完成该节点的配置。

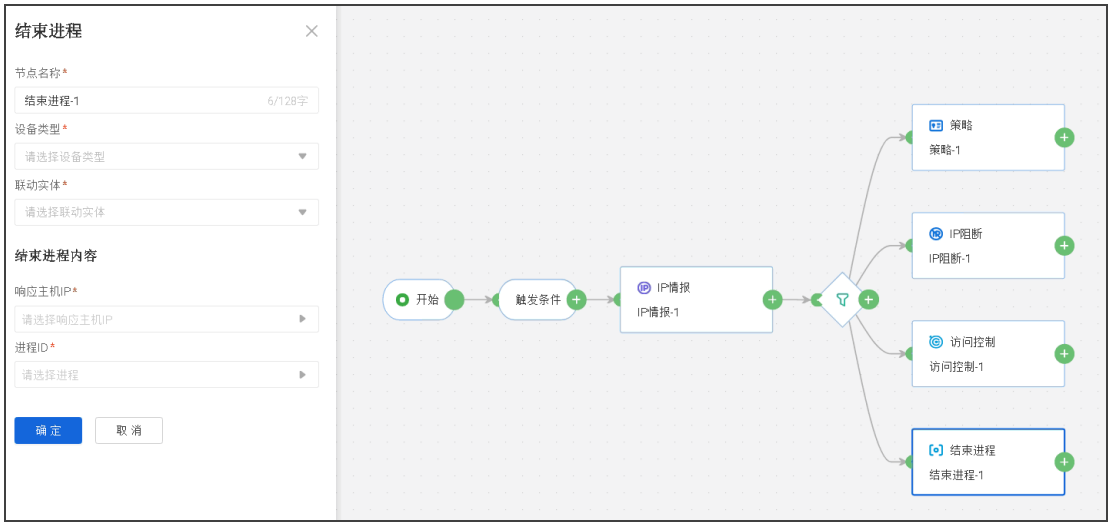
配置结束进程

配置响应的结束进程动作，请按照以下步骤进行操作：

1. 点击按钮，在<剧本模块>页面，点击主机安全设备动作“结束进程”。



2. 点击“确定”按钮，“结束进程”节点即添加至剧本拓扑图中。同时，左侧打开<结束进程>页面。



在<结束进程>页面，配置结束进程详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。
设备类型（必填项）	选择执行结束进程的设备类型。
联动实体（必填	选择结束进程需要关联的联动实体，点击下拉菜单选择已添加的主机

选项	说明
项）	安全设备实体。关于添加主机安全设备实体，请参阅添加主机安全设备实体。
结束进程内容	
响应主机IP（必填项）	点击下拉菜单，在打开的<这样主机IP>页面，指定这样的主机IP地址。例如，选择事件的源IP，即将对匹配触发条件的威胁事件源地址指定为这样的主机IP地址。
进程ID（必填项）	点击下拉菜单，在打开的<进程ID>页面，指定需要结束的进程ID。

3. 点击“确定”完成该节点的配置。

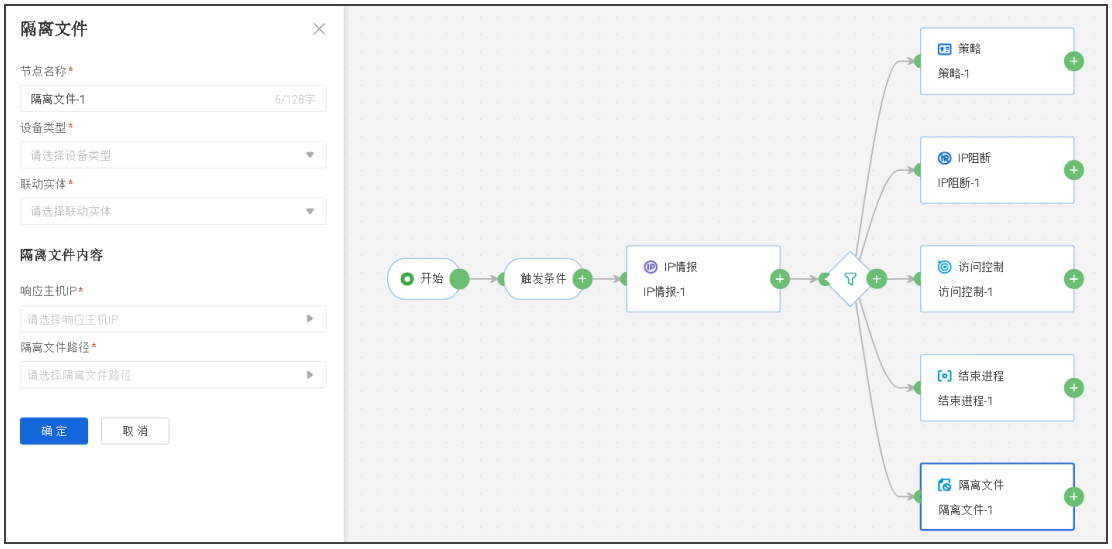
配置隔离文件

配置响应的隔离文件动作，请按照以下步骤进行操作：

1. 点击 按钮，在<剧本模块>页面，点击主机安全设备动作“隔离文件”。



2. 点击“确定”按钮，“隔离文件”节点即添加至剧本拓扑图中。同时，左侧打开<隔离文件>页面。



在<隔离文件>页面，配置隔离文件详细信息。

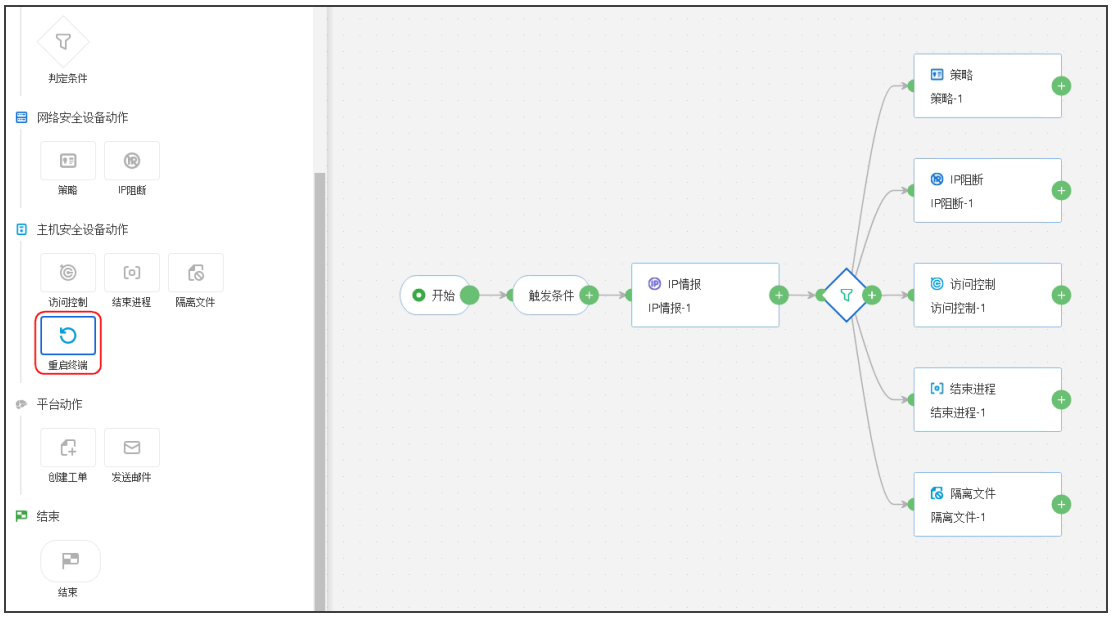
选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。
设备类型（必填项）	选择执行隔离文件的设备类型。
联动实体（必填项）	选择隔离文件需要关联的联动实体，点击下拉菜单选择已添加的主机安全设备实体。关于添加主机安全设备实体，请参阅添加主机安全设备实体。
隔离文件内容	
响应主机IP（必填项）	点击下拉菜单，在打开的<响应主机IP>页面，指定响应的主机IP地址。例如，选择事件的源IP，即将对匹配触发条件的威胁事件源地址指定为响应的主机IP地址。
隔离文件路径（必填项）	点击下拉菜单，在打开的<隔离文件路径>页面，指定被隔离的文件存储路径。例如，选择事件的文件路径，即将对匹配触发条件的威胁事件中指定路径下的运行的恶意程序的文件进行隔离。

3. 点击“确定”完成该节点的配置。

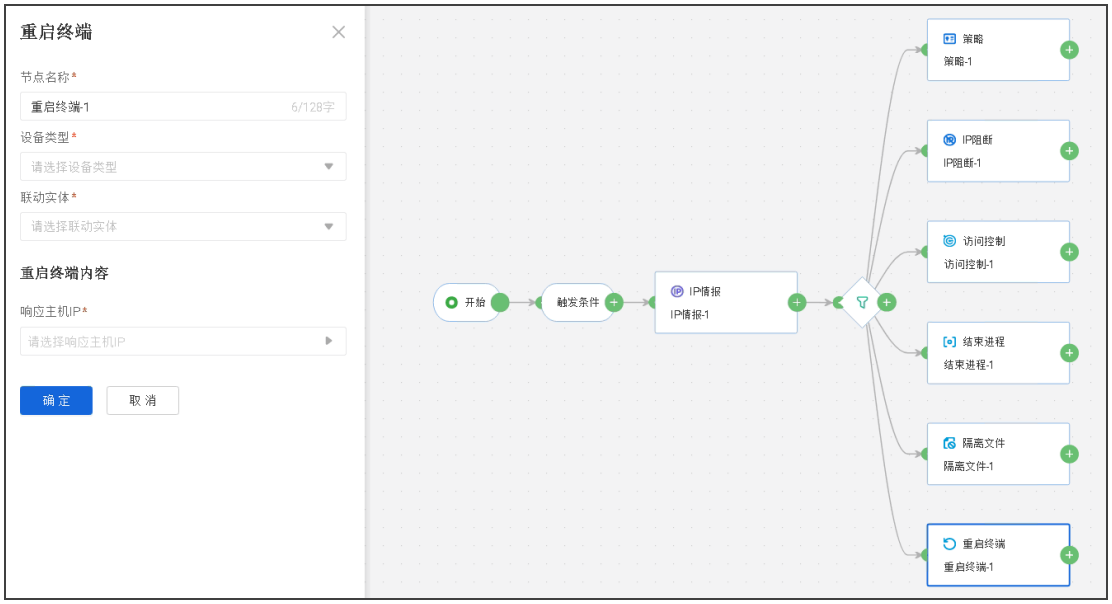
配置重启终端

配置响应的重启终端动作，请按照以下步骤进行操作：

1. 点击 按钮，在<剧本模块>页面，点击主机安全设备动作“重启终端”。



2. 点击“确定”按钮，“重启终端”节点即添加至剧本拓扑图中。同时，左侧打开<重启终端>页面。



在<重启终端>页面，配置重启终端详细信息。

选项	说明
节点名称（必填	指定剧本中该节点的名称，范围是1到128个字符。

选项	说明
项）	
设备类型（必填项）	选择执行重启终端的设备类型。
联动实体（必填项）	选择重启终端需要关联的联动实体，点击下拉菜单选择已添加的主机安全设备实体。关于添加主机安全设备实体，请参阅添加主机安全设备实体。
重启终端内容	
响应主机IP（必填项）	点击下拉菜单，在打开的<响应主机IP>页面，指定重启系统的主机IP地址。例如，选择事件的源IP，即将对匹配触发条件的威胁事件源地址指定为重启系统的主机IP地址。

3. 点击“确定”完成该节点的配置。

配置平台动作

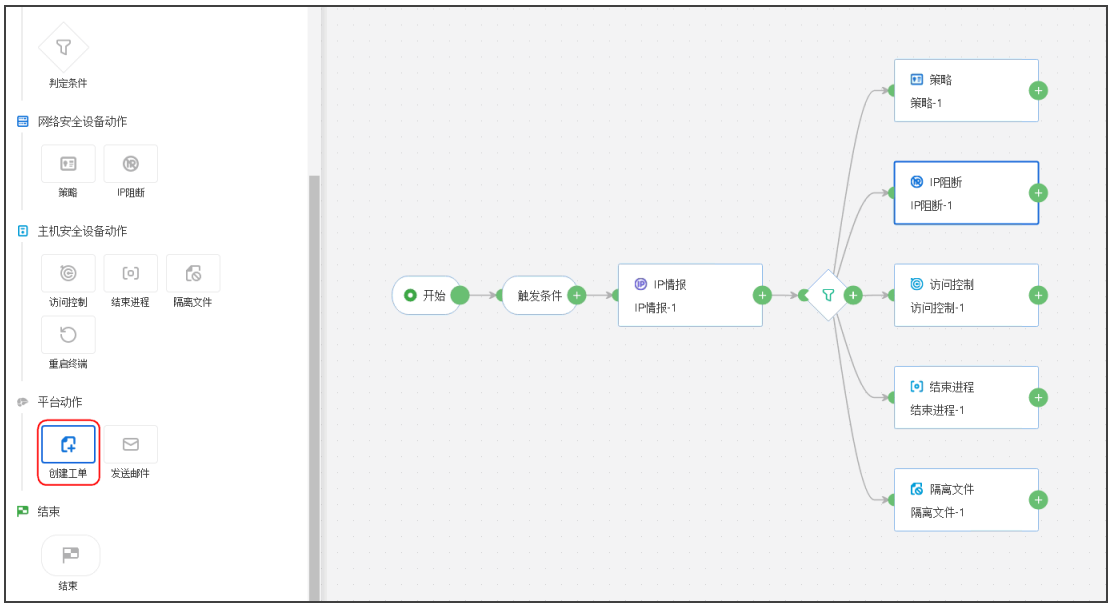
在剧本的编排中，需要指定智源平台对威胁事件执行的自动响应处理动作。自动化剧本将自动执行该响应处理动作，人工确认剧本需要人工确认是否执行该响应处理动作。

剧本中支持配置的平台动作有：创建工单、邮件通知。

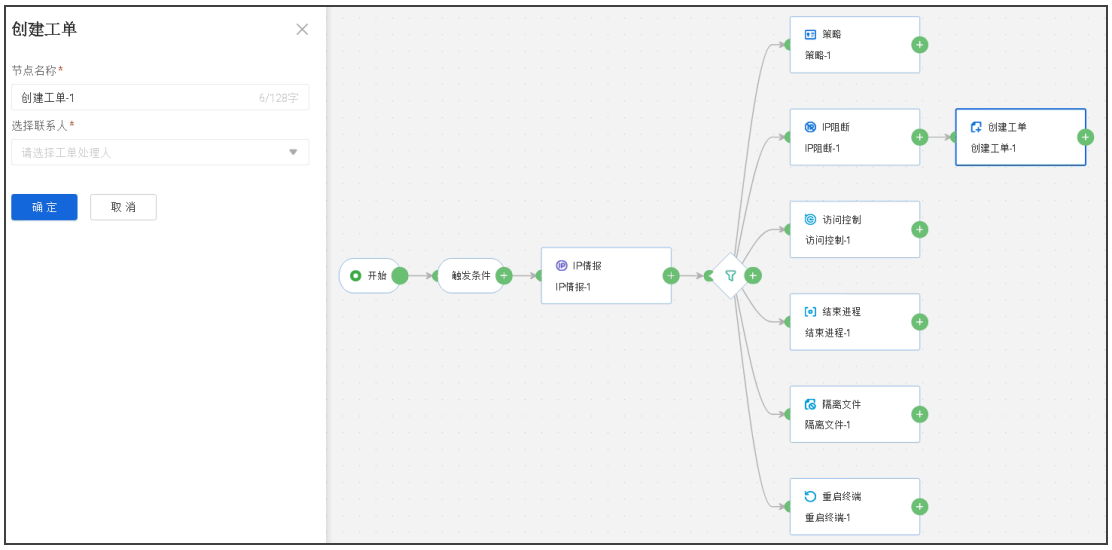
创建工单

配置响应下发的工单，请按照以下步骤进行操作：

1. 点击按钮，在<剧本模块>页面，点击平台动作“创建工单”。



2. 点击“确定”按钮，“创建工单”节点即添加至剧本拓扑图中。同时，左侧打开<创建工单>页面。



在<创建工单>页面，配置工单详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。

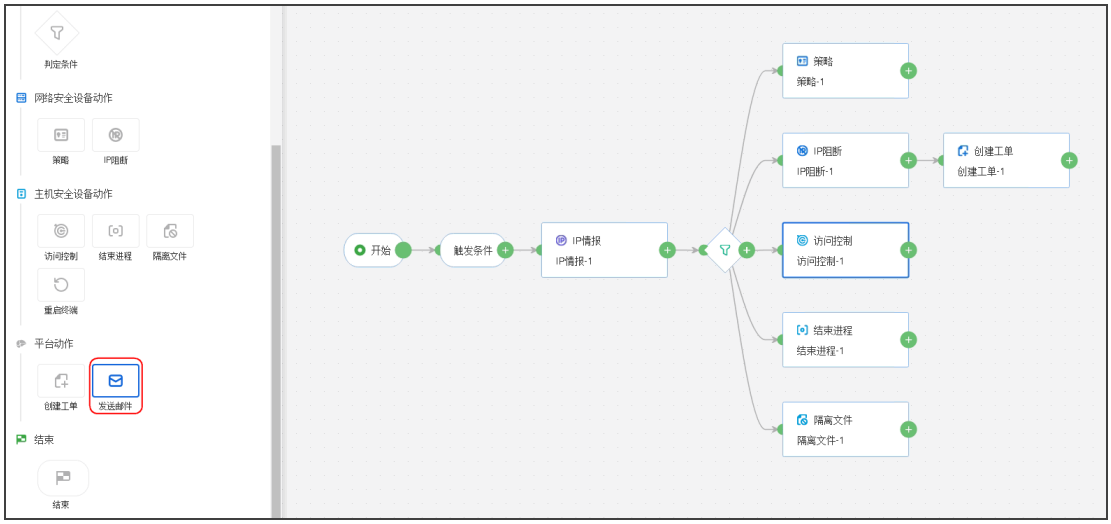
选项	说明
选择联系人（必填项）	点击下拉菜单打开联系人列表，选择工单的处理人，将会按照联系人的邮箱地址，以邮件形式将工单发送给指定联系人。 • 在搜索框中输入指定的联系人名称，点击搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“工单处理人”选项中已选择的工单处理人。 请先确保已配置好邮件服务器。关于邮件服务器的配置，请参阅"通讯配置" 在第469页。

3. 点击“确定”完成该节点的配置。

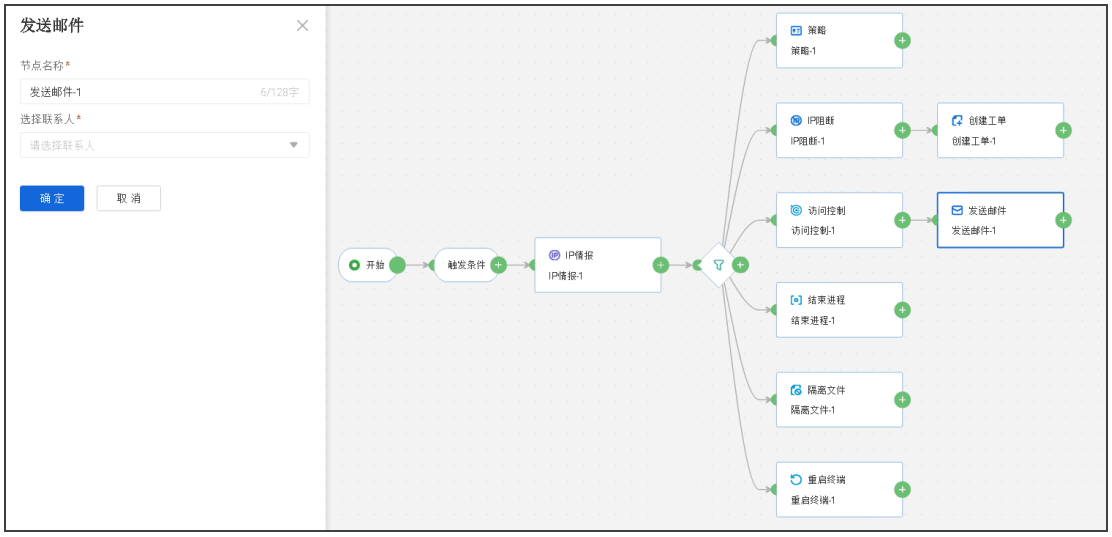
发送邮件

配置响应下发的邮件，请按照以下步骤进行操作：

1. 点击按钮，在<剧本模块>页面，点击平台动作“发送邮件”。



2. 点击“确定”按钮，“发送邮件”节点即添加至剧本拓扑图中。同时，左侧打开<发送邮件>页面。



在<发送邮件>页面，配置邮件详细信息。

选项	说明
节点名称（必填项）	指定剧本中该节点的名称，范围是1到128个字符。
选择联系人（必填项）	点击下拉菜单打开联系人列表，选择剧本执行后被通知的联系人，将会按照联系人的邮箱地址，以邮件形式将剧本执行后的通知发送给指定联系人。 • 在搜索框中输入指定的联系人名称，点击搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“选择联系人”选项中已选择的联系人。 请先确保已配置好邮件服务器。关于邮件服务器的配置，请参阅"通讯配置" 在第469页。

3. 点击“确定”完成该节点的配置。

联动实体

联动实体是指用于与智源平台联动处理威胁事件的网络安全设备、主机安全设备或威胁情报库。用户可以将联动实体添加至智源平台进行集中管理，对联动实体执行相关动作，实现在智源平台中快速跳转或下发响应配置至联动实体，以完成对威胁事件的手动响应处理或自动响应处理。

联动实体包含网络安全设备、主机安全设备和威胁情报库三种类型，目前支持和以下设备进行联动：

类型		介绍
网络安全设备	NGFW/IDPS	山石网科下一代防火墙（NGFW）与入侵检测和防御系统（IDPS） 支持多维度可视及精细化管控的功能，为用户提供L2-L7层网络的全面安全防护，具有丰富的部署场景和高性能业务体验。
	HSM	山石网科安全管理平台 能够实现山石安全设备的统一管理，支持安全设备集中监控、安全策略统一运维，配置集中管理等，可有效提升用户的运维管理效率。
	WAF	山石网科Web应用防火墙（WAF） 保护用户的网站及核心Web应用，提供从资产发现、漏洞评估、篡改监测、流量自学习、威胁定位到智能误报分析的一站式解决方案，对包括OWASP TOP10在内的各种应用层风险进行检测及减缓，同时针对加密流量和IPv6流量也具备完整的防护能力，确保网站和Web应用的全天候安全运行。
	ADC	山石网科应用交付AX系列 是新一代专业的应用交付产品，支持链路负载、服务器负载和全局负载功能，同时还提供缓存加速、IPv6代理、共计检测、SSL卸载、加密流量分析等扩展特性，可以大幅提高核心应用系统的可用性、可扩展性以及安全可视能力，有效提升企业数据中心的运营效率。
	云 · 界	山石云 · 界是专门为云计算环境设计的虚拟化网络安全产品。

类型		介绍
		内嵌山石网科StoneOS网络防火墙专用操作系统，以虚拟机形态部署，适用于云计算和虚拟化环境。产品支持精细化应用识别、VPN、入侵防御、病毒过滤、负载均衡等功能，可串联或单臂连接到虚拟网络中，为虚拟网络或应用提供专业的边界网络安全防护功能。
	云·格	山石云·格是一种提供虚拟机间东西向安全管控能力的云防火墙产品。 产品结合了NFV和SDN的优势，将网络微格离、安全可视化能力下沉至云内虚机的身边，提供“贴身保镖”式的、全方位的网络安全防护。山石云·格产品既是云计算零信任安全模型的最佳实践产品，又是Gartner推荐的主流云安全技术之一，并于2020年入选Gartner CWPP全球市场指南。
主机安全设备	山石云鉴主机安全管理系统	山石云鉴主机安全管理系统（CloudDis） 完善了等保整体解决方案中端点安全防护产品的布局，满足等保合规建设场景要求，具备对主机的基线核查、多维度风险监控、微隔离监控、多层级安全响应功能，可以防御内网中高发的勒索病毒、挖矿病毒等威胁。
威胁情报库	云瞻	山石云瞻提供一站式威胁情报分析服务。 威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，对威胁或危害的响应或处理决策提供信息支持。威胁情报主要内容为用于识别和检测威胁的失陷标识，如IP地址、域名、文件HASH等，以及相关的归属标签。
	VirusTotal	VirusTotal提供一站式威胁情报分析服务。 威胁情报是某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，对威胁或危害的响应或处理决策提供信息支持。威胁情报主要内容为用于识别和检测威胁的失陷标识，如IP地址、域名、URL、文件HASH等，以及相关的归属标签。

联动实体动作

网络安全设备支持以下联动动作：

- 登录： 一键跳转至联动实体设备的界面。
- 策略：配置策略实现控制安全域间/不同地址段间的流量转发。（仅NGFW/IDPS、云·界和云·格支持该动作）
- IP阻断：将IP添加到黑名单后，系统将对黑名单中的IP执行阻断操作，直到阻断时间结束。（仅NGFW/IDPS、云·界支持该动作）

主机安全设备支持以下联动动作：

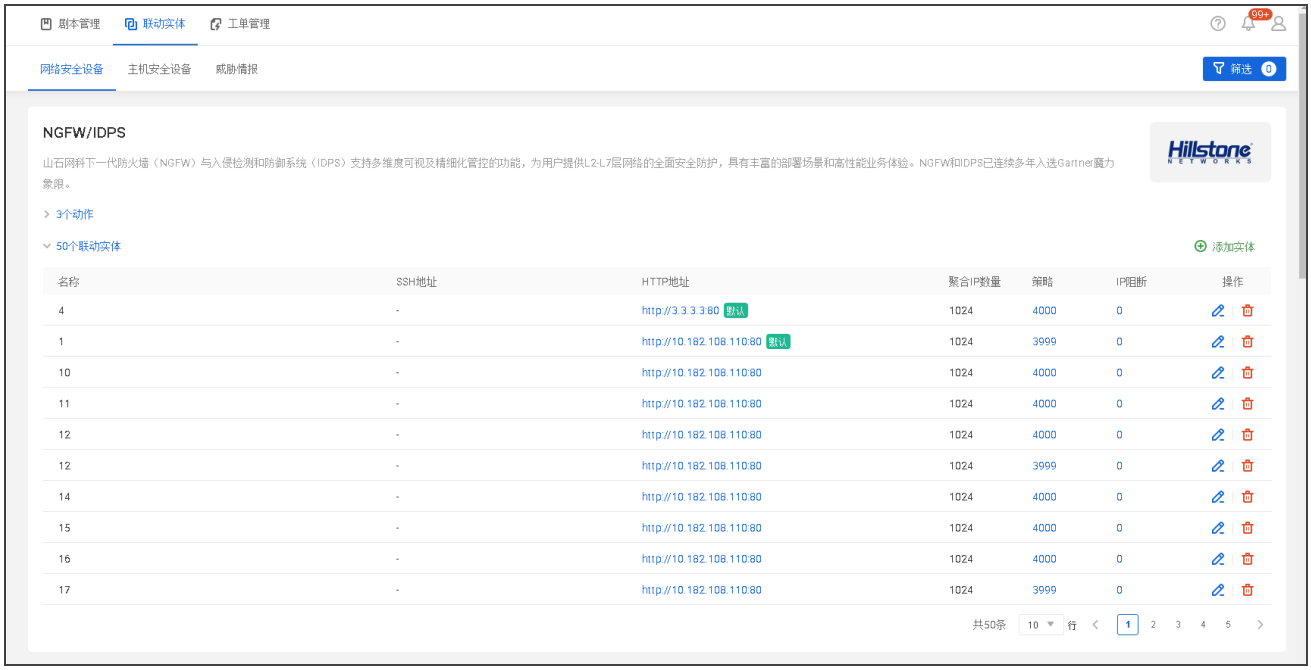
- 访问控制： 阻断指定主机与指定IP、端口、协议、方向的通信。
- 结束进程：结束指定主机的指定进程。
- 隔离文件：隔离指定主机的指定文件。
- 重启系统：重启指定主机的操作系统。
- USB白名单：将指定USB厂商标识添加到指定主机的USB白名单列表。
- 阻止非信任USB：阻止非信任USB接入指定主机。

威胁情报库支持以下联动动作：

- IP情报：查询指定IP地址的情报信息，对威胁或危害的响应或处理决策提供信息支持。
- 域名情报：查询指定域名的情报信息，对威胁或危害的响应或处理决策提供信息支持。
- 文件情报：查询指定文件的情报信息，对威胁或危害的响应或处理决策提供信息支持。
- URL情报：查询指定URL网址的情报信息，对威胁或危害的响应或处理决策提供信息支持。（仅VirusTotal支持该动作）

网络安全设备

点击“事件响应>联动实体”，打开联动实体页面，点击<网络安全设备>标签页，打开网络安全设备联动实体页面。



- 在右上角筛选条件中指定网络安全设备类别、名称或者地址，网络安全设备联动实体页面将按照筛选条件展示对应联动实体。
- 网络安全设备联动实体卡片中展示了厂商信息、设备名称、设备简介、支持的联动动作、已添加的联动实体列表。
- 在网络安全设备联动实体卡片中，点击“X个动作”，展开所选网络安全设备支持的所有联动动作。
- 在网络安全设备联动实体卡片中，点击“X个联动实体”，展开对应该网络安全设备所有已添加的联动实体列表。
- 在网络安全设备联动实体卡片中，点击“添加实体”按钮，添加对应该网络安全设备类型的联动实体。具体配置方式，请参阅添加网络安全设备实体。
- 在已展开的联动实体列表中，可以执行以下操作：
  - 点击“地址”/“HTTP地址”列中的地址信息，将会在浏览器中打开新的网页，打开指定的网络安全设备的WebUI页面。
  - 点击“策略”列中的数字，打开当前所选联动实体详情页面，在下方列表<策略>标签页中查看当前联动实体已经执行过的策略列表。点击数字后的 按钮，配置策略。详细配置方法，请参阅配置策略。

- 点击“IP阻断”列中的数字，打开当前所选联动实体详情页面，在下方列表<IP阻断>标签页中查看当前联动实体已经执行过的IP阻断列表。点击数字后的 按钮，配置IP阻断。详细配置方法，请参阅配置IP阻断。
- 点击“操作”列的  按钮，打开<编辑实体>页面，可以修改联动实体配置信息。
- 点击“操作”列的  按钮，删除所选联动实体。

添加网络安全设备实体

在智源平台中添加网络安全设备实体，请按照以下步骤进行操作：

1. 点击“事件响应>联动实体”，选择<网络安全设备>标签页，打开网络安全设备联动实体页面。

2. 选择需要添加的网络安全设备类型，在对应卡片中点击“添加实体”按钮，打开<添加实体>页面。


添加实体
名称 *
请输入名称
0/128字
SSH地址
地址
请输入SSH地址
22
用户名
请输入用户名
密码
请输入密码
HTTP地址
地址
http
请输入IP或URL
80
用户名
请输入用户名
密码
请输入密码
默认联动方式
默认动作
SSH地址
HTTP地址
剧本下发策略聚合配置
聚合IP数量
1024
默认为1024，支持配置16-1024
确定
测试
取消

在“添加实体”页面，填写联动的网络安全设备实体配置信息。

选项	说明
名称（必填项）	指定网络安全设备实体的名称。 长度为0到128个字符。
SSH地址	
地址	指定网络安全设备实体的SSH地址以及端口号，用于访问联动实体设备的CLI页面。
用户名	指定登录网络安全设备实体系统CLI页面的用户名。
密码	指定登录网络安全设备实体系统CLI页面的用户名对应的密码。
HTTP地址	
地址	指定网络安全设备实体的地址以及端口号，用于访问联动实体设备的WebUI页面。点击下拉菜单选择http或https方式，然后在文本框中输入IP地址或URL地址以及端口号。
用户名	指定登录网络安全设备实体系统WebUI页面的用户名。
密码	指定登录网络安全设备实体系统WebUI页面的用户名对应的密码。
默认联动方式	
默认动作	指定与网络安全设备实体的默认联动方式，使用SSH地址或者使用HTTP地址。
剧本下发策略聚合配置（仅NGFW/IDPS、云·界、云·格支持）	
聚合IP数量	剧本中为联动实体自动下发的策略规则支持根据源IP、目的IP、源安全域、 目的安全域以及服务进行聚合。 当自动下发的策略规则源安全域、 目的安全域以及服务相同且满足以下条件时，均会自动聚合： • 新策略与原有策略是子集关系； • 新策略与原有策略是超集关系；

选项	说明
	• 新策略与原有策略的源IP或者目的IP不同，其他配置相同。 在根据源IP、目的IP聚合下发的策略规则时，“聚合IP数量”表示单条策略规则支持聚合的源IP个数或者目的IP个数。默认值为1024，范围是16-1024。 **注意**: • 在指定“聚合IP数量”时，请根据联动实体中策略规则的IP数目进行配置，不允许超过允许配置的最大值。 • 如果剧本下发的策略被聚合，将会在剧本响应记录详情中展示。

3. 点击“测试”按钮，测试添加的网络安全设备实体连通性。
4. 点击“确定”按钮，完成配置。同时，系统将会对已配置的网络安全设备实体进行连通性测试。



注意:

- 网络安全设备联动实体支持免认证登录。当用户完成网络安全设备实体的配置后，在跳转至对应联动实体设备的页面时，可使用已指定的用户名密码实现免认证登录。
- 如果免认证登录失败，将会跳转至对应网络安全设备联动实体设备的登录页面，用户输入登录用户名和密码即可完成登录。

查看网络安全设备实体策略/IP阻断信息

在网络安全设备联动实体列表中，点击“策略”或“IP阻断”列中的数字，打开当前所选联动实体详情页面。



- 页面上方展示网络安全设备联动实体的基本信息，下方展示网络安全设备联动实体已执行的策略和IP阻断列表。
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的策略规则/IP阻断条目。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击<策略>标签页，查看当前联动实体已经执行的策略列表，包括已执行策略的“名称”、“源安全域”、“源IP”、“目的安全域”、“目的IP”、“服务”、“动作”、“下发方式”、“下发主体”、“下发时间”、“开始时间”、“结束时间”、“循环周期”、“状态”和“操作”。
  - 自动剧本下发的策略“下发主体”列显示剧本的名称，点击剧本名称，查看剧本的详细信息；手动下发或人工确认剧本下发的策略“下发主体”列显示下发人的账号。
  - 未到“开始时间”的策略状态为“待生效”，在“开始时间”和“结束时间”内的策略状态为“生效中”，超过“结束时间”的策略状态为“已失效”；在“循环周期”内策略状态为“生效中”，在“循环周期”外的策略状态为“待生效”。
  - 点击“配置策略”按钮，配置联动实体需要执行的策略规则。具体配置方式，请参阅配置策略。
- 点击<IP阻断>标签页，查看当前联动实体已经执行的IP阻断列表，包括已执行IP阻断的“虚拟路由器”、“阻断IP”、“下发方式”、“下发主体”、“开始时间”、“结束时间”、“状态”和“操作”。

    - 自动剧本下发的IP阻断“下发主体”列显示剧本的名称，点击剧本名称，查看剧本的详细信息；手动下发过人工确认剧本下发的IP阻断“下发主体”列显示下发人的账号。
    - “开始时间”和“结束时间”列决定IP阻断的状态。在时间周期内的IP阻断状态为“正常”；超过结束时间的IP阻断状态为“失效”。
    - 点击“配置IP阻断”按钮，配置联动实体需要执行的IP阻断。具体配置方式，请参阅配置IP阻断。
- 点击列表中指定策略规则/IP阻断条目的 按钮，删除所选策略规则/IP阻断条目。如需批量删除，勾选多个策略规则/IP阻断条目，点击列表右上角的“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新策略列表/IP阻断列表。

配置策略

配置网络安全设备联动实体需要执行的策略规则，请按照以下步骤进行操作：

1. 在网络安全设备联动实体详情页面中，点击<策略>标签页，打开策略列表。

2. 点击“配置策略”按钮，打开<配置策略>页面。



在“配置策略”页面，配置策略规则信息。

选项	说明
策略名称（必填项）	指定策略规则的名称。 最多支持配置95个英文字符或31个中文字符。
IP地址类型（必填项）	指定策略规则IP地址的类型，默认为IPv4类型。指定IP类型后，配置源、目的IP地址时只能填写相应类型的IP地址。
生效时间（必填项）	指定策略的生效时间，可以选择“永久有效”、“固定时间”或“周期循环”。 • 选择“永久有效”，则该策略一直处于生效状态。

选项	说明
	• 选择“固定时间”，配置策略生效的“开始时间”和“结束时间”，精确到小时，可以只配置“开始时间”或“结束时间”。未到“开始时间”的策略状态为“待生效”；在“开始时间”和“结束时间”内的策略状态为“生效中”；超过“结束时间”的策略状态为“已失效”。 • 选择“周期循环”，选择循环的周期和起止时间，循环周期可选择每周的某一天，可多选。精确到小时。处于“循环周期”内的策略状态为“生效中”；在“循环周期”外的策略状态为“待生效”。
源安全域（必填项）	指定策略规则的源安全域。
源IP（必填项）	指定策略规则的源地址。 • 选择“Any”，表示选择任意源地址。 • 选择“自定义”后，选择“IP/掩码”或“IP范围”，并在下方文本框中输入源地址，然后点击“添加”按钮，表示该策略规则对指定源地址生效。 **注意**: • 当配置IPv6类型的地址时，不支持配置IPv4映射IPv6地址（如::ffff:1.1.1.1）或者格式类似于::ffff:12:34的IPv6地址。 • 最多支持配置的源地址个数与网络安全设备实体配置中“聚合IP数量”一致。
目的安全域（必填项）	指定策略规则的源安全域。
目的IP（必填项）	指定策略规则的目的地址。 • 选择“Any”，表示选择任意目的地址。

选项	说明
	• 选择“自定义”后，选择“IP/掩码”或“IP范围”，并在下方文本框中输入源地址，然后点击“添加”按钮，表示该策略规则对指定目的地址生效。 **注意**： • 当配置IPv6类型的地址时，不支持配置IPv4的映射地址（如::ffff:1.1.1.1）或者格式类似为::ffff:12:34的地址，否则会出现错误。 • 最多支持配置的目的地址个数与网络安全设备实体配置中“聚合IP数量”一致。
服务（必填项）	指定策略规则的服务。 • 选择“Any”，表示选择任意服务。 • 选择“自定义”点击“添加服务规则”按钮，并在指定协议类型、目的端口号和源端口号，然后点击“确定”按钮，完成添加服务规则。 **注意**：系统允许最多添加32个服务规则。
动作（必填项）	指定对匹配策略规则的流量所采取的行为，包括允许和拒绝。

3. 点击“确定”按钮，完成策略规则的配置。

配置IP阻断

配置网络安全设备联动实体需要执行的IP阻断，请按照以下步骤进行操作：

1. 在网络安全设备联动实体详情页面中，点击<IP阻断>标签页，打开IP阻断列表。

2. 点击“配置IP阻断”按钮，打开<配置IP阻断>页面。



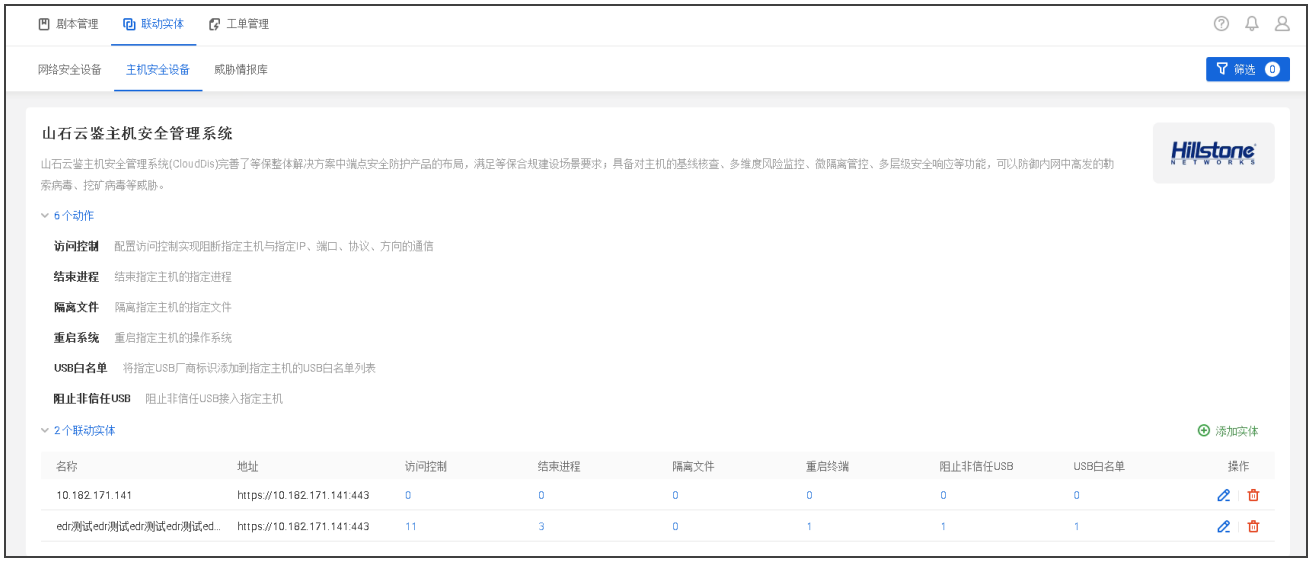
在“配置IP阻断”页面，配置IP阻断信息。

选项	说明
虚拟路由器（必填项）	在下拉菜单中选择被阻断IP所属的虚拟路由器。
IP地址类型（必填项）	指定阻断的IP地址类型，并在文本框中输入需要被阻断的IP。 此IP地址既可以为发起访问的源IP地址， 也可以为被访问的目的IP地址。
阻断时长（必填项）	在文本框中输入IP地址将被阻断的时长， 单位为分钟， 范围是1到1440分钟。

3. 点击“确定”按钮，完成IP阻断的配置。

主机安全设备

点击“事件响应>联动实体 ”，打开联动实体页面，点击<主机安全设备>标签页，打开主机安全设备联动实体页面。



- 在右上角筛选条件中指定主机安全设备类别、名称或者地址，主机安全设备联动实体页面将按照筛选条件展示对应联动实体。
- 主机安全设备联动实体卡片中展示了厂商信息、设备名称、设备简介、支持的联动动作、已添加的联动实体列表。
- 在主机安全设备联动实体卡片中，点击“X个动作”，展开所选主机安全设备支持的所有联动动作。
- 在主机安全设备联动实体卡片中，点击“X个联动实体”，展开对应该主机安全设备所有已添加的联动实体列表。
- 在主机安全设备联动实体卡片中，点击“添加实体”按钮，添加对应该主机安全设备类型的联动实体。具体配置方式，请参阅添加主机安全设备实体。
- 在已展开的联动实体列表中，可以执行以下操作：
  - 点击“访问控制”/“结束进程”/“隔离文件”/“重启终端”/“阻止非信任USB”/“USB白名单”列中的数字，打开当前所选联动实体详情页面，在下方列表<访问控制>/<结束进程>/<隔离文件>/<重启终端>/<阻止非信任USB>/<USB白名单>标签页中查看当前联动实体已经执行过的动作列表。点击数字后的 按钮，配置对应的联动动作。
  - 点击“操作”列的 按钮，打开<编辑实体>页面，可以修改联动实体配置信息。
  - 点击“操作”列的 按钮，删除所选联动实体。

添加主机安全设备实体

在智源平台中添加主机安全设备实体，请按照以下步骤进行操作：

1. 点击“事件响应>联动实体”，选择<主机安全设备>标签页，打开主机安全设备联动实体页面。
2. 选择需要添加的主机安全设备类型，在对应卡片中点击“添加实体”按钮，打开<添加实体>页面。



在“添加实体”页面，填写联动的主机安全设备实体配置信息。

选项	说明
名称（必填项）	指定主机安全设备实体的名称。 长度为0到128个字符。
地址	指定主机安全设备实体的地址以及端口号，用于下发联动动作。在文本框中输入IP地址或URL地址以及端口号。

3. 点击“测试”按钮，测试添加的主机安全设备实体连通性。
4. 点击“确定”按钮，完成配置。同时，系统将会对已配置的主机安全设备实体进行连通性测试。

查看主机安全设备实体详情信息

在主机安全设备联动实体列表中，点击“访问控制”/“结束进程”/“隔离文件”/“重启终端”/“阻止非信任USB”/“USB白名单”列中的数字，打开当前所选联动实体详情页面。



- 页面上方展示主机安全设备联动实体的基本信息，下方展示主机安全设备联动实体已执行的访问控制/结束进程/隔离文件/重启终端/阻止非信任USB/USB白名单列表。
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的访问控制/结束进程/隔离文件/重启终端/阻止非信任USB/USB白名单条目。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击<访问控制>/<结束进程>/<隔离文件>/<重启终端>/<阻止非信任USB>/<USB白名单>标签页，查看当前联动实体已经执行的动作列表。自动剧本下发的动作“下发主体”列显示剧本名称；手动下发或人工确认剧本下发的动作“下发主体”列显示下发人的账号。
- 在各标签页中，点击“配置访问控制”/“配置结束进程”/“配置隔离文件”/“配置重启终端”/“配置阻止非信任USB”/“配置USB白名单”按钮，配置联动实体需要执行动作。
- 点击列表中指定动作条目的 按钮，删除所选动作条目。如需批量删除，勾选多个动作条目，点击列表右上角的“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新详情信息列表。

配置访问控制

访问控制用来阻断指定主机与指定IP、端口、协议、流量方向的通信。

配置主机安全设备联动实体需要执行的访问控制，请按照以下步骤进行操作：

1. 在主机安全设备联动实体详情页面中，点击<访问控制>标签页，打开访问控制条目列表。

2. 点击“配置访问控制”按钮，打开<新增访问控制>页面。



在“新增访问控制”页面，配置访问控制信息。

选项	说明
响应主机IP（必填项）	在文本框中输入响应的主机IP地址。
阻断远端IP（必填项）	在文本框中输入需要被阻断的远端IP地址，阻断响应主机与该远端IP之间的通信。
阻断协议（必填项）	点击下拉菜单选择需要被阻断的协议类型。
阻断目的端口（必填项）	在文本框中输入需要被阻断的目的端口号，阻断响应主机与该目的端口之间的通信。
阻断流量方向	点击“入站”或“出站”单选按钮，指定阻断流量方向。 • 入站：阻断远端IP对响应主机的访问。

选项	说明
	• 出站：阻断响应主机对远端IP的访问。

3. 点击“确定”按钮，完成访问控制的配置。

配置结束进程

结束进程用来结束指定主机的指定进程。

配置主机安全设备联动实体需要执行的结束进程动作，请按照以下步骤进行操作：

1. 在主机安全设备联动实体详情页面中，点击<结束进程>标签页，打开结束进程条目列表。
2. 点击“配置结束进程”按钮，打开<新增结束进程>页面。



在“新增结束进程”页面，配置结束进程信息。

选项	说明
响应主机IP（必填项）	在文本框中输入响应的主机IP地址。
进程ID（必填项）	在文本框中输入需要结束的进程ID。

3. 点击“确定”按钮，完成结束进程的配置。

配置隔离文件

隔离文件是指隔离指定主机的指定文件。

配置主机安全设备联动实体需要执行的隔离文件动作，请按照以下步骤进行操作：

1. 在主机安全设备联动实体详情页面中，点击<隔离文件>标签页，打开隔离文件条目列表。
2. 点击“配置隔离文件”按钮，打开<新增隔离文件>页面。



在“新增隔离文件”页面，配置隔离文件信息。

选项	说明
响应主机IP（必填项）	在文本框中输入响应的主机IP地址。
隔离文件路径（必填项）	在文本框中输入需要被隔离的文件存储路径。

3. 点击“确定”按钮，完成隔离文件的配置。

配置重启终端

重启终端是指重启指定主机设备的操作系统。

配置主机安全设备联动实体需要执行的重启终端动作，请按照以下步骤进行操作：

1. 在主机安全设备联动实体详情页面中，点击<重启终端>标签页，打开重启终端条目列表。
2. 点击“配置重启终端”按钮，打开<重启终端>页面。



在“新增重启终端”页面，配置重启终端信息。

选项	说明
响应主机IP（必填项）	在文本框中输入需要重启系统的主机IP地址。

3. 点击“确定”按钮，完成重启终端的配置。

配置阻止非信任USB

阻止非信任USB是指阻止非信任USB接入到指定主机。该动作仅支持手动配置以及响应，不支持在剧本中配置。

配置主机安全设备联动实体需要执行的阻止非信任USB动作，请按照以下步骤进行操作：

1. 在主机安全设备联动实体详情页面中，点击<阻止非信任USB>标签页，打开阻止非信任USB条目列表。
2. 点击“配置阻止非信任USB”按钮，打开<新增阻止非信任USB>页面。



在“新增阻止非信任USB”页面，配置阻止非信任USB信息。

选项	说明
响应主机IP（必填项）	在文本框中输入需要响应的主机IP地址，将会阻止非信任USB接入到该主机中。

3. 点击“确定”按钮，完成阻止非信任USB的配置。

配置USB白名单

USB白名单是指将指定USB厂商标识添加到指定主机的USB白名单列表，添加后该USB厂商的USB将会被作为信任USB。该动作仅支持手动配置以及响应，不支持在剧本中配置。

配置主机安全设备联动实体的USB白名单，请按照以下步骤进行操作：

1. 在主机安全设备联动实体详情页面中，点击<USB白名单>标签页，打开USB白名单条目列表。
2. 点击“配置USB白名单”按钮，打开<新增USB白名单>页面。



在“新增USB白名单”页面，配置USB白名单信息。

选项	说明
响应主机IP（必填项）	在文本框中输入需要响应的主机IP地址。
USB厂商（必填项）	输入USB厂商标识信息，格式为：VID_XXX或者VID_XXX&PID_XXX，然后点击“添加”按钮。 查询USB厂商标识信息方法如下： 1. 打开“我的电脑>属性>设备管理器”，打开设备管理器页面。 2. 选择“通用串行总线控制器”，在设备管理器页面中找到目标USB设备。 3. 点击鼠标右键选择“属性”，然后选择“详细信息”标签页。 4. 在“属性”下拉菜单中选择“硬件Id”，在“值”列表中复制对应的VID或者PID部分内容。

3. 点击“确定”按钮，完成USB白名单的配置。

威胁情报库

点击“事件响应>联动实体 ”，打开联动实体页面，点击<威胁情报库>标签页，打开威胁情报库联动实体页面。



- 在右上角筛选条件中指定联动实体类别或名称，威胁情报库联动实体页面将按照筛选条件展示对应联动实体。
- 威胁情报库联动实体卡片中展示了厂商信息、设备名称、设备简介、支持的联动动作、已添加的联动实体列表。
- 点击“查询情报”按钮，将会在浏览器中打开新的网页，打开对应的威胁情报平台页面，用于手动查询威胁情报。
- 在威胁情报库联动实体卡片中，点击“X个动作”，展开所选威胁情报库支持的所有联动动作。
- 在威胁情报库联动实体卡片中，点击“X个联动实体”，展开对应该威胁情报库所有已添加的联动实体列表。
- 在威胁情报库联动实体卡片中，点击“添加实体”按钮，添加对应该威胁情报库类型的联动实体。具体配置方式，请参阅添加威胁情报库实体。
- 在已展开的联动实体列表中，可以执行以下操作：
  - 点击“操作”列的按钮，打开<编辑实体>页面，可以修改联动实体配置信息。
  - 点击“操作”列的 按钮，删除所选联动实体。

添加威胁情报库实体

在智源平台中添加威胁情报库实体，请按照以下步骤进行操作：

1. 点击“事件响应>联动实体”，选择<威胁情报库>标签页，打开威胁情报库联动实体页面。
2. 选择需要添加的威胁情报库类型，在对应卡片中点击“添加实体”按钮，打开<添加实体>页面。



在“添加实体”页面，填写联动实体配置信息。

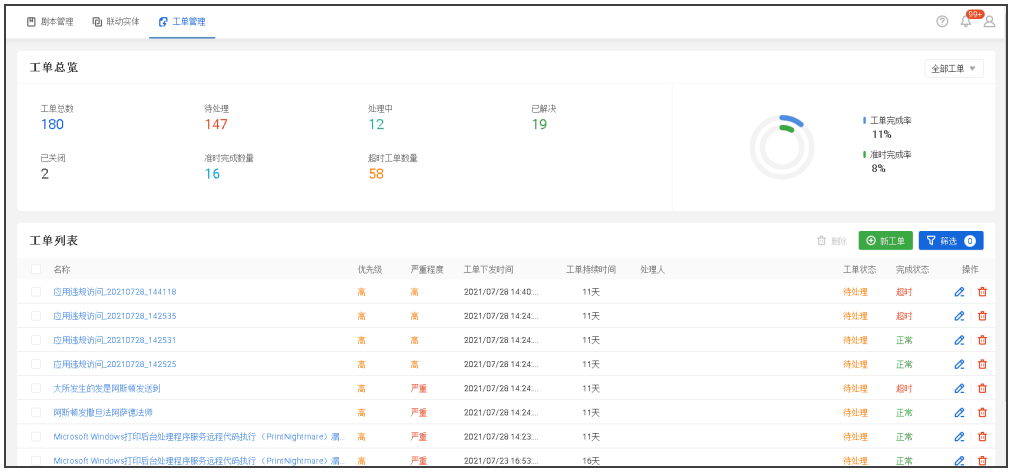
选项	说明
名称（必填项）	指定联动实体的名称。 长度为0到128个字符。
API 地址	该API地址是指访问威胁情报服务平台的地址，用于查询威胁情报。不可编辑，仅可查看。
API Key（必填项）	API Key是指用来访问威胁情报服务平台的授权信息码。 当用户在威胁情报服务平台中完成注册或购买威胁情报服务之后，威胁情报服务平台将会提供给用户该API Key（注册用户仅提供试用 API Key，购买服务后将提供正式API Key），用户在智源平台中添加实体时，即可指定该API Key以保证能够正常访问对应的威胁情报服务平台。

3. 点击“确定”按钮，完成配置。

工单管理

对威胁事件手动响应过程中，如果某个威胁事件需要通过下发工单与其他人进行协作处理和跟踪，用户可以在工单管理页面中配置对应的工单，将该威胁事件或相关风险资产需要实施的处理通知到指定处理人。

点击“事件响应>工单管理”，打开工单管理页面。



- 在“工单总览”部分，查看工单的数量统计结果，包括工单总数、待处理工单数、处理中的工单数、已解决工单数、已关闭工单数、准时完成数量、超时工单数量，以及以环形图形式展示了工单完成率和工单准时完成率。
    - 点击对应的数字，系统将根据工单状态及完成状态作为筛选条件筛选对应的工单，显示在页面下方的工单列表中。
- 点击“工单总览”部分右上角“全部工单”下拉菜单指定工单的处理人，“工单总览”部分将会按照指定处理人展示对应处理人的工单统计总览结果。
- “工单列表”部分展示所有已创建的工单。
- 点击列表中的“名称”链接，查看所选工单的工单详情。
- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的工单。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击工单列表中工单条目后的 按钮，打开“编辑工单”页面，编辑所选工单。

- 点击工单列表中工单条目后的  按钮，删除所选工单。如需批量删除工单，勾选多个工单条目，点击“删除”按钮。
- 点击页面左下角  按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角  按钮，刷新工单列表。

新建工单

新建工单，请按照以下步骤进行操作：

1. 点击“事件响应>工单管理”，打开工单管理页面。

2. 在“工单列表”部分，点击“新工单”按钮，打开“新工单”页面。



在“新工单”页面，填写工单基本配置信息。

选项	说明
工单名称（必填项）	指定工单的名称。 长度为0到128个字符。
优先级（必填项）	指定工单优先级，包括高、中、低。优先级越高的工单，将会被优先处理。

选项	说明
严重程度（必填项）	指定工单的严重程度，包括严重、高、中、低。用户可以根据工单的严重程度决定处理工单的优先顺序。
工单处理人	点击下拉菜单打开联系人列表，选择工单的处理人，将会按照联系人的邮箱地址，以邮件形式将工单发送给指定联系人。 • 在搜索框中输入指定的联系人名称，点击 搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“工单处理人”选项中已选择的工单处理人。 请先确保已配置好邮件服务器。关于邮件服务器的配置，请参阅"通讯配置" 在第469页。
相关资产	在下拉菜单指定资产类型，再选择需要处理的对应服务器或终端。
限时完成	点击时间选择框，指定工单处理的限定最晚完成时间。通过该指定时间来判定工单的准时完成率。
问题描述	指定工单处理的问题的描述信息。
处理意见	指定工单的处理意见。
处理记录	指定工单的处理操作历史记录。

3. 点击“确定”按钮完成配置。

查看工单详情

在工单管理页面点击列表中的“名称”链接，查看所选工单的工单详情，如下图所示。



该页面提供以下内容：

- 显示该工单的工单名称、工单状态、严重程度、优先级、邮件通知邮箱地址、限时完成时间、相关资产、资产所属人、工单处理人、完成时间、问题详细描述、处理意见、处理记录及工单日志。
- 若该工单由剧本自动生成，在“问题详细描述”部分显示：“当前工单由剧本XXX生成，由XXX威胁事件触发，请立即处理。”点击剧本名称或威胁事件名称，可查看对应剧本的详细或查看该威胁事件的详细信息。
- 在用户新建该工单或编辑该工单后，系统将会生成工单日志。工单日志中记录了对该工单的操作记录，包括执行操作的用户名、操作时间、以及执行的操作内容。
- 点击页面右上角的“编辑”按钮，可对该页面中除了工单日志以外的内容进行编辑。

第7章 报告管理

系统为用户提供报告管理功能，包括报告和等保管理。

- 综合展示网络风险概况，包括综合评分、威胁概览、风险服务器/终端安全概况和趋势以及工单概览，为用户呈现全方位、多角度的统计报告。用户可通过报告模板制定报告任务，生成对应的报告，在报告总览页面中查看生成的报告文件。
- 对等级保护建设整改过程中产生的报告以及其他相关信息进行统计归档，并使用可视化的统一界面进行展现与管理。

报告管理部分包含如下内容：

- "报告总览" 在第287页：介绍查看已生成的报告文件。
- "报告任务" 在第290页：介绍如何新建报告任务以及查看已经创建的报告任务。
- "报告模板" 在第293页：介绍报告模板类型以及如何查看报告模板的详细信息。
- "等保管理" 在第300页：介绍如何使用等级保护工作管理工具。

报告总览

用户可以在报告总览页面查看已生成的报告文件。点击“报告报告>报告总览”，打开报告总览页面。



- 按照报告生成时间，展示所有已生成的报告文件，最新生成的报告在列表最上方。
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的报告文件。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击列表中报告文件条目“操作”列中的 按钮，下载PDF格式或Word格式的报告文件。
- 点击列表中报告文件条目“操作”列中的 按钮，在打开页面中在线查看报告文件。详报不可在线查看。
- 点击列表中报告文件条目“操作”列中的 按钮，删除该报告文件。如需批量删除报告文件，勾选多个报告文件条目，点击页面右上角的“删除”按钮。
- 已读报告文件名称在列表中将显示为灰色。
- 点击“生成报告”按钮，新建临时报告任务，立即生成报告文件。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新报告总览页面列表中的报告文件。

生成报告

用户可以根据需要新建临时报告任务，立即生成报告文件。

立即生成报告文件，请按照以下步骤进行操作：

1. 点击“报告管理>报告总览”。

2. 点击页面右上角的“生成报告”按钮，打开<生成报告>页面。



在<生成报告>页面，填写临时报告任务基本配置信息。

选项	说明
任务名称（必填项）	指定临时报告任务的名称。
报告模板（必填项）	点击下拉菜单，选择需要使用的报告模板。
报告形式（必填项）	勾选报告的呈现形式，包括简报和详报，可多选。简报展示风险概况，详报展示风险的详细信息。
开始时间	指定报告数据采集周期的开始时间。
结束时间	指定报告数据采集周期的结束时间。
描述	指定临时报告任务的描述信息。



注意: 新建的临时报告任务不会在报告任务列表中显示。

报告任务

报告任务是与报告生成有关的时间计划，它规定报告文件使用的名称、报告模板、报告形式、报告类型、以及生成时间。

当设备恢复出厂设置或升级后不包含任何报告任务时，系统将会预置3个报告任务，分别是：服务器安全风险报告简报、终端安全风险报告简报、综合安全风险报告简报的周报任务，以上预置报告任务仅作为报告任务的样例，可以编辑和删除。同时，用户还可以在设备上按照需求配置自定义报告任务，生成报告文件。

点击“报告管理>报告任务”，打开报告任务页面，查看已经创建的报告任务列表。



- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的报告任务。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击报告任务条目“状态”列的按钮，启用或禁用该报告任务。表示报告任务状态为已启用，表示报告任务状态为禁用。
- 点击报告任务条目中的按钮，打开“详情”页面，查看所选报告任务的详细信息，如报告模板、报告类型等。
- 点击报告任务条目中的按钮，打开“编辑报告任务”页面，编辑所选报告任务。也可以在“详情”页面，点击“编辑”按钮，同样可以编辑该报告任务。
- 点击报告任务条目中的按钮，删除所选报告任务。
- 点击“新任务”，新建报告任务。

新建报告任务

新建报告任务，请按照以下步骤进行操作：

1. 点击“报告管理>报告任务”。

2. 点击页面右上角“新任务”按钮，打开<新报告任务>页面。



在<新报告任务>页面，填写报告任务基本配置信息。

选项	说明
任务名称（必填项）	指定报告任务的名称。
报告类型（必填项）	指定报告的类型，根据指定周期内的数据生成报告，包括日报、周报、月报、季报和年报。 **注意**: • 当指定为季报或年报时，报告模板仅支持选择预定义报告模板，且不可指定生成时间。 • 季报的统计时间范围为1-3月、4-6月、7-9月、10-12月，生成时间默认为4月、7月、10月和次年1月第一天的6点。 • 年报的统计时间范围为1-12月，生成时间默认为次年1月3日的6点。

选项	说明
生成时间	指定生成报告文件的时间。
报告模板（必填项）	点击下拉菜单，选择需要使用的报告模板。
报告形式（必填项）	勾选报告的呈现形式，包括简报和详报，可多选。简报展示风险概况，详报展示风险的详细信息。
消息通知	点击“启用”按钮，开启/关闭消息通知功能。 开启该功能，并点击下拉菜单打开联系人列表，选择指定收件人，可多选。当报告生成后，系统将会以邮件形式将报告文件发送到指定收件人。 • 在搜索框中输入指定的联系人名称，点击 搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在打开的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空选项中已选择的收件人。
描述	指定报告任务的描述信息。

3. 点击“确定”按钮完成配置。

报告模板

报告模板是报告文件的基础，要生成报告文件，需要首先配置报告模板，报告模板规定报告文件的统计内容。

报告模板包括报告Logo、默认模板和自定义模板。

- 报告Logo：用户可按照需求修改报告模板上的Logo和文案，修改后将应用到所有的报告模板。
- 默认模板：即系统内置报告模板，不可编辑或删除。包括如下默认报告模板：

类别	说明
综合安全风险报告	综合展示网络风险概况，包括综合评分、风险服务器/终端概况、威胁概览、弱点概览以及工单概览。
终端安全风险报告	综合展示终端的安全情况和趋势，以及所有风险终端的威胁标签、威胁事件和弱点。
服务器安全风险报告	综合展示服务器的安全情况和趋势，以及所有风险服务器的所属业务、威胁标签、威胁事件和弱点。
事件响应报告	综合展示工单的分布情况和趋势，以及所有工单的名称、优先级、下发时间、持续时间、处理人和状态信息。

基于默认模板生成的报告分为简报和详报。简报展示风险概况，详报展示风险的详细信息。用户可以在新建临时报告任务或新建报告任务时指定生成简报或详报。具体默认模板对应简报和详报展示的内容如下表所示：

类别	说明
综合安全风险简报	综合展示网络风险概况，包括综合评分、风险服务器/终端概况、威胁概览、弱点概览以及工单概览。
终端安全风险简报	综合展示终端安全风险概况，包括风险终端的安全状态分布、风险统计及Top10列表。
终端安全风险详报	综合展示终端安全情况和趋势，以及风险终端详情，包括风险终端的IP地址、风险等级、威胁数量、弱点数量、资产价值、所属区域、威胁标签、威胁来源Top5、威胁事件及弱点。

类别	说明
服务器安全风险简报	综合展示服务器安全风险概况，包括风险服务器的安全状态分布、风险统计及Top10列表。
服务器安全风险详报	综合展示服务器安全情况和趋势，以及风险服务器详情，包括风险服务器的IP地址、风险等级、威胁数量、弱点数量、资产价值、所属区域、所属业务、威胁标签、威胁来源Top5、威胁事件及弱点。
事件响应简报	综合展示工单统计概况，包括工单完成统计及工单趋势。
事件响应详报	综合展示工单分布情况和趋势以及工单列表，包括工单的名称、优先级、下发时间、持续时间、处理人和状态信息。

- 自定义报告模板：用户可按照需求创建自定义报告模板，对模板的名称、标签颜色、描述和报告内容进行选择与配置。系统最多允许创建10个自定义报告模板。

注意: 综合安全风险报告模板仅支持生成简报。

自定义报告Logo

上传自定义Logo和文案后将替换报告模板上页眉和页脚处的Logo和文案，同时隐藏报告首页顶部默认的“Hillstone”图案。自定义报告模板上的Logo和文案，请按照以下步骤进行操作：

1. 选择“报告管理>报告模板”，进入报告模板页面。
2. 在报告Logo区域，点击按钮，打开<自定义报告Logo>页面。



在<自定义报告Logo>页面，填写相关配置信息。

选项	说明
上传Logo	上传自定义Logo。图片支持PNG格式，大小不超过1M，尺寸建议为120*120。默认为智源智能安全运营系统的Logo。
自定义文案（必填项）	指定Logo后的文案。最多允许输入64个字符。默认为“山石网科智源智能安全运营系统”。

3. 点击“确定”按钮，完成配置。

4. 如需恢复默认配置，点击<自定义报告Logo>页面左下角“恢复默认”按钮。

注意: 用户自定义的Logo和文案将会应用到所有报告模板中，但不影响已生成的报告。

查看报告模板详情

查看报告模板详情，请按照以下步骤进行操作：

1. 选择“报告管理>报告模板”，进入报告模板页面。

2. 点击所选报告模板面板中的 按钮，打开<详情>页面，查看所选报告模板的详细信息，如名称、服务器、终端、工单、统计内容、区域和描述等。

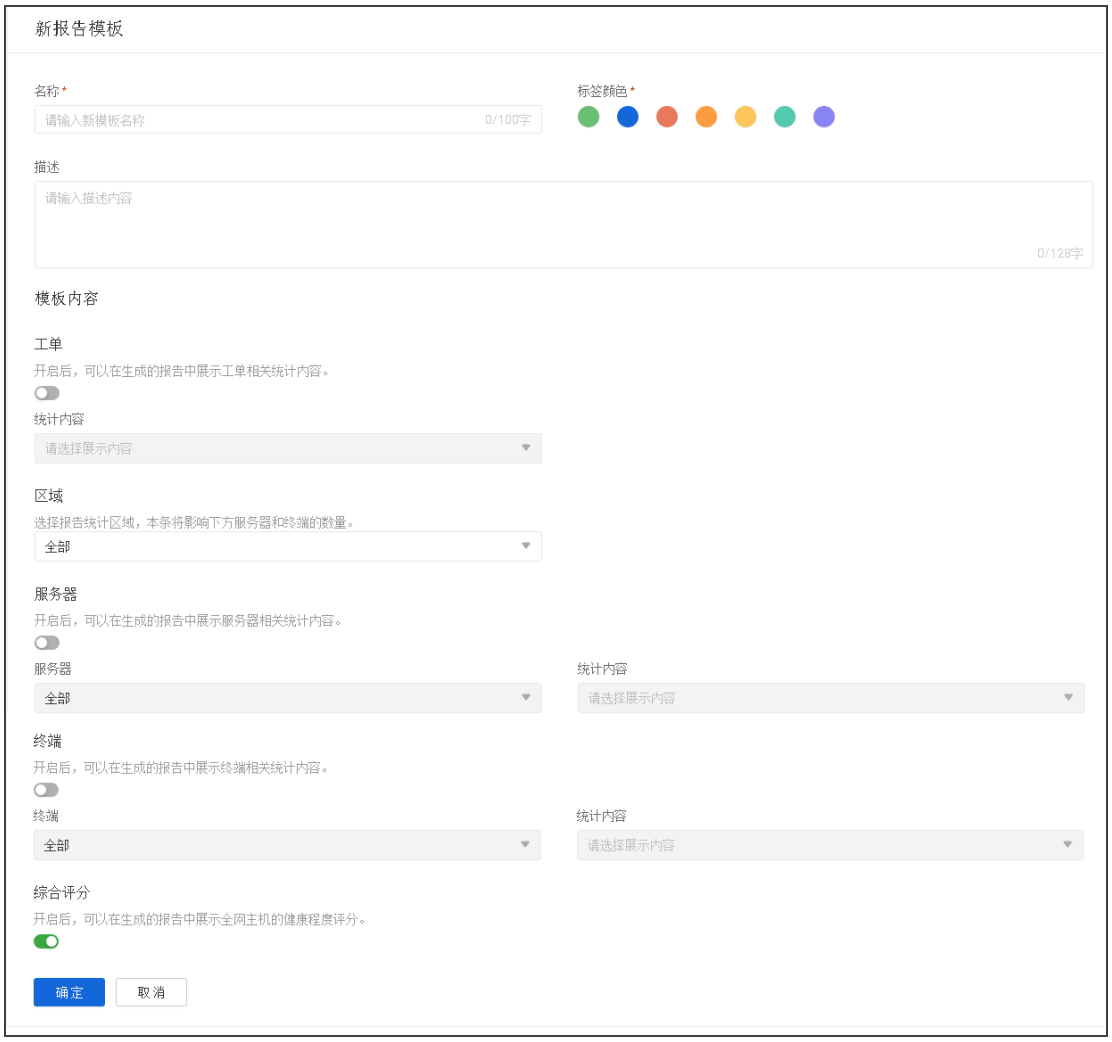


新建自定义报告模板

新建自定义报告模板，请按照以下步骤进行操作。

1. 选择“报告管理>报告模板”，进入报告模板页面。

2. 在自定义模板区域，点击“新模板”，打开<新报告模板>页面。



在<新报告模板>页面，填写相关配置信息。

选项	说明
名称（必填项）	指定自定义模板的名称。保存配置后，用户无法进行更改。
标签颜色（必填项）	指定自定义模板的标签颜色。
描述	指定对自定义模板的描述信息。
模板内容	
工单	点击启用按钮，在生成报告中展示工单相关统计内容。 开启后，在“统计内容”下拉列表中勾选工单数据的展示内容，包括工单分布图、折线趋势图和工单列表，可多选。
区域	在下拉列表中勾选数据所属的区域，可多选。若不勾选，默认选择全部区域。 **注意**：可选的服务器和终端将会受所选区域的影响。
服务器	点击启用按钮，在生成报告中展示服务器相关统计内容。 开启后，在“服务器”下拉列表中勾选需要统计的服务器名称，可多选，如不勾选，则默认选择全部服务器；在“统计内容”下拉列表中勾选服务器数据的展示内容，包括饼状分布图、折线趋势图，风险服务器Top10列表、威胁详情列表、弱点详情列表，可多选。
终端	点击启用按钮，在生成报告中展示终端相关统计内容。 开启后，在“终端”下拉列表中勾选需要统计的终端名称，可多选，如不勾选，则默认选择全部终端；在“统计内容”下拉列表中勾选终端数据的展示内容，包括饼状分布图、折线趋势图，风险终端Top10列表、威胁详情列表、弱点详情列表，可多选。
综合评分	点击启用按钮，在生成报告中展示全网主机的健康程度评分。

3. 点击“确认”按钮，完成配置。

编辑自定义报告模板

编辑自定义报告模板，请按照以下步骤进行操作：

1. 选择“报告管理>报告模板”，进入报告模板页面。
2. 在自定义模板区域，点击所选自定义报告模板面板中的 按钮，打开<编辑报告模板>页面，对所选模板进行编辑。也可以在“详情”页面，点击“编辑”按钮，同样可以编辑该报告任务。
3. 编辑完成后，点击“确定”按钮完成配置。

删除自定义报告模板

删除自定义报告模板，请按照以下步骤进行操作：

1. 选择“报告管理>报告模板”，进入报告模板页面。
2. 在自定义模板区域，点击所选自定义报告模板面板中的 按钮。也可以勾选所需自定义报告模板右上角的复选框，然后点击自定义模板区域右上角的 按钮。
3. 在弹出的对话框中点击“确定”，删除所选自定义报告模板。

等保管理

等保，即是网络安全等级保护，是指对国家重要信息、法人和其他组织及公民的专有信息以及公开信息、存储/传输/处理这些信息的信息系统分等级实行安全保护。等级保护的工作流程包括6个阶段：定级、备案、自查、整改、等级测评、监督检查，在等级保护工作的每个环节中，都需要对当前环节产生的相关信息进行管理。

智源提供等保管理功能，为用户的等级保护工作提供了一种管理工具。针对用户在等级保护建设整改过程中产生的报告以及其他相关信息进行统计归档，并使用可视化的统一界面进行展现与管理。

等保系统

等保系统就是等级保护对象，是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成，并且按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

等保系统中包含对应的资产和等保流程。用户可以在智源平台中完成以下配置：

- 创建等保系统
- 编辑等保系统
- 删除等保系统
- 管理资产
- 管理等保流程
- 查看等保系统/流程

创建等保系统

在智源平台中创建等保系统，请按照以下步骤进行操作：

1. 选择“报告管理>等保管理”，进入等保管理页面。
2. 点击“新等保系统”按钮，打开<新等保系统>页面。



在<新等保系统>页面，填写等保系统基本信息。

选项	说明
系统名称（必填项）	指定等保系统的名称。
备注	指定等保系统的备注信息。

3. 点击“确定”按钮，保存配置。

编辑等保系统

在智源平台中编辑已创建的等保系统，请按照以下步骤进行操作：

1. 选择“报告管理>等保管理”，进入等保管理页面。
2. 在需要编辑的等保系统面板中，点击右上角的 按钮，打开<编辑等保系统>页面，对所选等保系统基本信息进行编辑。
3. 编辑完成后，点击“确定”按钮完成配置。

删除等保系统

在智源平台中删除已创建的等保系统，请按照以下步骤进行操作：

1. 选择“报告管理>等保管理”，进入等保管理页面。
2. 在需要删除的等保系统面板中，点击右上角的 按钮。如需批量删除等保系统，勾选多个等保系统左上角的复选框或者勾选“全选”，然后点击页面右上角的“删除”按钮。
3. 在弹出的对话框中点击“确定”，删除所选等保系统。



注意: 当删除一个等保系统时，该等保系统中包含的等保流程均会被一同删除。

管理资产

每个等保系统中均需要包含对应的资产，用户可以在等保系统中通过填写资产信息来创建新资产，还可以将资产信息从本地导入到等保系统中。

创建新资产

创建新资产，请按照以下步骤进行操作：

1. 在已创建完成的等保系统页面中，点击“资产数量”部分的“管理资产”，打开资产页面。

2. 点击“新资产”按钮，打开<新资产>页面。



在<新资产>页面，填写添加至等保系统的资产信息。

选项	说明
IP地址（必填项）	指定资产的IP地址。目前仅支持IPv4类型的IP地址。
设备类型	指定资产的类型，网络设备或者安全设备。
资产编号	指定资产的固定编号。
操作系统	点击下拉菜单选择添加的资产对应的操作系统类型。
数据库	点击下拉菜单选择添加的资产对应的数据库类型。

选项	说明
描述	指定添加的资产的描述信息。

3. 点击“确定”按钮，添加的资产即可显示在列表中。

导入资产

用户可以将资产信息从本地导入到等保系统中。导入前，建议下载模板文件，并在.csv格式的模板文件中填写等保系统资产信息。

下载模板

下载模板文件，查看标准的等保系统资产信息文件格式。模板内容如下图所示：

# 等保系统资产CSV文件模板						
IP地址	设备类型	资产编号	操作系统	数据库	描述	

下载等保系统资产信息的模板文件，请按照以下步骤进行操作：

1. 在已创建完成的等保系统页面中，点击“资产数量”部分的“管理资产”，打开资产页面。
2. 点击左下角“下载模板”按钮，下载格式为.csv的模板文件。

导入资产

在本地按照模板文件格式和内容填写资产信息后，导入等保系统，请按照以下步骤进行操作：

1. 点击“导入”按钮，打开<导入资产>页面。
2. 点击“选择文件”，选择所需导入的文件。选择后若需更换文件，点击“取消”按钮。
3. 点击“上传”按钮。
    - 若文件通过系统校验，则弹出导入进度条，完成导入。
    - 若文件未通过系统校验，则显示“导入文件失败”及错误信息。

管理等保流程

等保管理流程，是指对等保系统的等级保护工作流程，包括6个阶段：定级、备案、自查、整改、等级测评、监督检查。每一个等保系统可以包含一个或多个等保管理流程，最多允许创建100个等保流程。

创建等保流程

创建新等保流程，请按照以下步骤进行操作：

1. 在已创建完成的等保系统页面中，点击“新流程”，打开<新等保流程>页面。
2. 在“流程名称”文本框中输入等保管理流程的名称。
3. 点击“确定”按钮，完成等保流程的创建。

编辑等保流程

等保流程创建完成后，用户可以随着等保系统等级保护建设整改过程的进行，配置流程的各个阶段内容。



注意: 等保流程中的6个阶段存在约束关系，在前一个阶段记录完成后，才能进行至下一个阶段。

定级阶段

等保流程的定级阶段，主要目标是按照国家有关管理规范和定级标准，确定等保系统及其安全保护等级，并组织专家评审。用户可以在智源平台中记录等保流程定级阶段的安全等级、报告和专家评审意见。

编辑定级阶段，请按照以下步骤进行操作：

1. 在已创建的等保系统中，点击“X个等保流程”，展开所有等保流程列表。

2. 点击“定级”处的按钮，打开<定级>页面。



在<定级>页面，记录定级阶段的相关内容。

选项	说明
安全等级（必填项）	点击下拉菜单选择当前等保系统确定的安全等级。 安全等级包括以下级别： • 一级：S1A1G1 ； • 二级：S1A2G2、S2A2G2、S2A1G2； • 三级：S1A3G3、S2A3G3、S3A3G3、S3A2G3、S3A1G3； • 四级：S1A4G4、S2A4G4、S3A4G4、S4A4G4、S4A3G4、S4A2G4、S4A1G4；

选项	说明
	• 五级：S1A5G5、S2A5G5、S3A5G5、S4A5G5、S5A4G5、S5A3G5、S5A2G5、S5A1G5。 其中，S表示信息安全类等级，保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求；A表示系统服务保证类等级，保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求；定级对象的安全保护等级由信息安全类等级和系统服务保证类等级的较高者决定，G = MAX（S，A）。
定级报告	
时间	指定定级报告的更新时间。
报告	点击 按钮，选中本地保存的定级报告文件，然后点击“确定”按钮。 **注意**：报告格式必须为非可执行文件类型。
专家评审意见	在文本框中输入定级阶段专家评审后的意见内容。

3. 点击“确定”按钮，保存记录。

备案阶段

等保流程的备案阶段，是指等保系统在定级后，需要报备公安机关备案审查，办理备案手续。用户可以在智源平台中记录等保流程备案阶段的备案时间和报告。

编辑备案阶段，请按照以下步骤进行操作：

1. 点击“备案”处的按钮，打开<备案>页面。



在<备案>页面，记录备案阶段的相关内容。

选项	说明
时间	指定备案的时间。
报告	点击 按钮，选中本地保存的用于备案的报告文件，然后点击“确定”按钮。 **注意**：报告格式必须为非可执行文件类型。

2. 点击“确定”按钮，保存记录。

自查阶段

等保流程的自查阶段，是通过对等保系统的安全状态进行自查，总结高风险项，为等保系统的持续改进过程提供依据和建议。用户可以在智源平台中记录等保流程自查阶段的自查时间、自查分数、报告以及高风险项。

编辑自查阶段，请按照以下步骤进行操作：

1. 点击“自查”处的按钮，打开<自查>页面。



在<自查>页面，记录自查阶段的相关内容。

选项	说明
时间	指定自查的时间。
分数	输入自查阶段评定的分数，范围是1-100分。
报告	点击 按钮，选中本地保存的自查阶段产生的报告文件， 然后点击“确定”按钮。 **注意**：报告格式必须为非可执行文件类型。
高风险项	添加高风险项目：

选项	说明
	1. 点击“添加”按钮。 2. 在表格中高风险项文本框输入高风险项内容，并在“状态”下拉菜单中选择处理状态。 3. 点击按钮，保存添加的高风险项条目。 4. 如需删除高风险项条目，点击按钮。

2. 点击“确定”按钮，保存记录。

整改阶段

等保流程的整改阶段，是根据自查阶段的高风险项记录、处理以及整改建议进行建设整改，以确保等保系统的安全保护能力满足相应等级安全要求。用户可以在智源平台中记录等保流程整改阶段的整改时间以及整改报告。

编辑整改阶段，请按照以下步骤进行操作：

1. 点击“整改”处的按钮，打开<整改>页面。



在<整改>页面，记录整改阶段的相关内容。

选项	说明
时间	指定整改的时间。

选项	说明
报告	点击 按钮，选中本地保存的用于整改的报告文件，然后点击“确定”按钮。 **注意**：报告格式必须为非可执行文件类型。

2. 点击“确定”按钮，保存记录。

等级测评阶段

等保流程的等级测评阶段，是指网络安全等级测评机构对已经完成等级保护建设的等保系统定期进行的等级测评，确保等保系统的安全保护措施符合相应等级的安全要求。用户可以在智源平台中记录等保流程等级测评阶段得出的测评结论、测评报告以及反馈的高风险项。

编辑等级测评阶段，请按照以下步骤进行操作：

1. 点击“等级测评”处的按钮，打开<等级测评>页面。



在<等级测评>页面，记录等级测评阶段的相关内容。

选项	说明
时间	指定等级测评的时间。
结论	点击下拉菜单选择等级测评的结论，包括符合、基本符合或者不符合。

选项	说明
分数	输入等级测评阶段评定的分数，范围是1-100分。
报告	点击 按钮，选中本地保存的等级测评阶段产生的报告文件，然后点击“确定”按钮。 **注意**：报告格式必须为非可执行文件类型。
高风险项	添加高风险项目： 1. 点击“添加”按钮。 2. 在表格中高风险项文本框输入高风险项内容，并在“状态”下拉菜单中选择处理状态。 3. 点击 按钮，保存添加的高风险项条目。 4. 如需删除高风险项条目，点击 按钮。

2. 点击“确定”按钮，保存记录。

监督检查阶段

等保流程的监督检查阶段，是等级保护管理部门按照国家、行业相关等级保护监督检查要求及标准，对等保系统开展监督检查工作。用户可以在智源平台中记录等保流程监督检查阶段的检查时间以及报告。

编辑监督检查阶段，请按照以下步骤进行操作：

1. 点击“监督检查”处的按钮，打开<监督检查>页面。



在<监督检查>页面，记录监督检查阶段的相关内容。

选项	说明
时间	指定监督检查的时间。
报告	点击 按钮，选中本地保存的用于监督检查的报告文件，然后点击“确定”按钮。 **注意**：报告格式必须为非可执行文件类型。

2. 点击“确定”按钮，保存记录。

删除等保流程

删除等保流程，请按照以下步骤进行操作：

1. 在已创建的等保系统中，点击“X个等保流程”，展开所有等保流程列表。
2. 选择需要删除的等保流程，点击“操作”列的按钮。
3. 在<提示>对话框中点击“确定”按钮，完成删除。

查看等保系统/流程

选择“报告管理>等保管理”，进入等保管理页面，查看所有已创建的等保系统以及对应的等保流程。列表中，查看已创建的等保流程。



- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的等保系统。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 每个等保系统面板中展示该等保系统的当前等级、当前进行中的等保流程阶段、资产总数、以及所有等保流程。
- 等保流程中已完成的阶段将显示图标，点击该图标可查看该阶段的记录。
- 等保流程的“自查”、“等级测评”阶段如存在未处理状态的高风险项目，将会显示图标。
- 点击等保流程条目后的按钮，可对等保流程的名称进行编辑修改。

第8章 情报中心

威胁情报是一种基于证据的知识，主要内容为用于识别和检测威胁的标识，如DNS域名、IP地址、恶意代码等，旨在对威胁的响应或处理决策提供信息支持。

威胁情报分为预定义威胁情报（通过威胁情报库获取的威胁情报）和自定义威胁情报（加入白名单、黑名单的情报）。

情报中心页面以威胁情报为核心，配合热点威胁资讯展示、威胁情报库管理、配置自定义威胁情报功能，能够让用户全方面的了解威胁情报，智源平台可以根据情报生成对应的威胁规则，并根据这些威胁规则检出威胁事件，进而采取相应的响应处理。

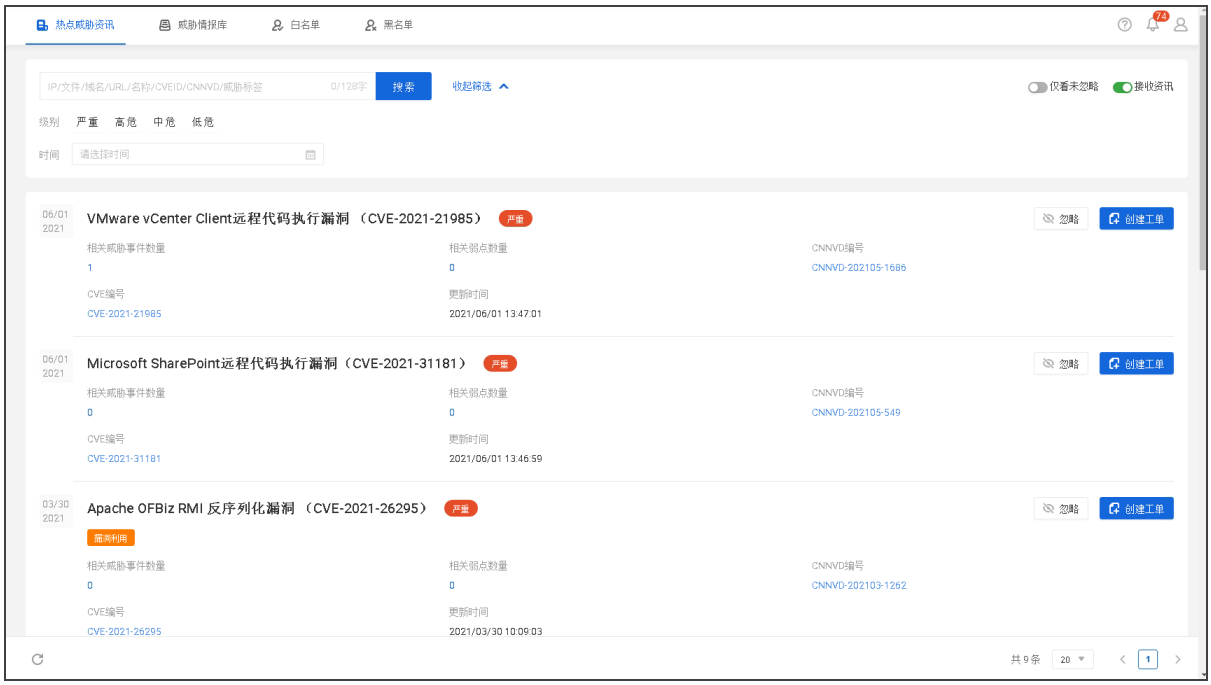
情报中心包含如下内容：

- "热点威胁资讯" 在第317页：介绍热点威胁情报展示内容以及相关响应操作。
- "威胁情报库" 在第320页：介绍威胁情报库的升级方法。
- "自定义威胁情报管理" 在第321页：介绍自定义白名单情报和黑名单情报的展示和添加方式。

热点威胁资讯

热点威胁资讯页面显示从山石云瞻威胁情报中心中获取的所有热点威胁情报信息。用户可以查看热点威胁情报的详细信息，也可对需要重点关注的威胁情报下发工单进行协作处理和跟踪，从而对热点威胁进行防范。

选择“情报中心 > 热点威胁资讯”，进入热点威胁情报页面。热点威胁情报列表显示从山石云瞻威胁情报中心中获取的所有热点威胁情报信息。



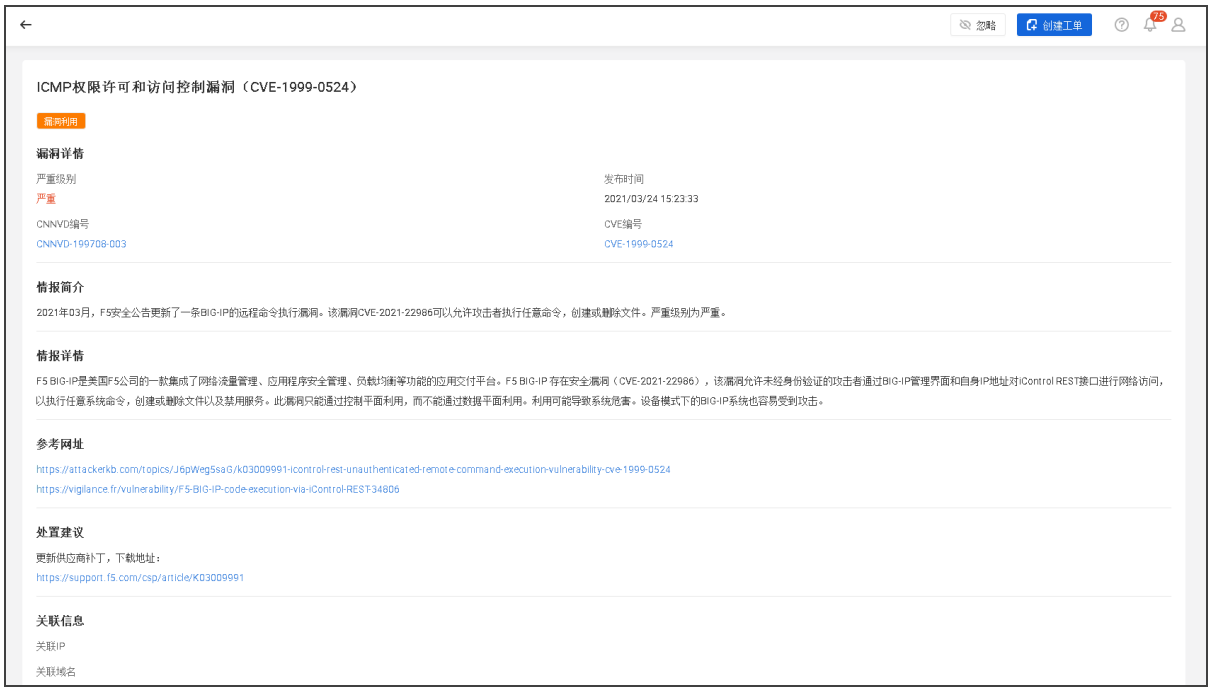
- 在搜索框输入“IP/文件名称/域名/URL/威胁情报名称/CVEID/CNNVD/威胁标签”对应内容，点击“搜索”可筛选符合条件的威胁情报信息。或者在筛选条件中指定严重级别、指定威胁情报生成的时间段来筛选符合条件的威胁情报信息。
- 点击“仅看未忽略”前的启用按钮，列表中将会仅展示未忽略的热点威胁情报信息，已忽略的将隐藏。
- 点击“接收资讯”前的启用按钮，山石云瞻威胁情报中心将会向智源平台推送最新的热点情报，同时智源平台收到后，将会自动更新热点威胁资讯列表。如未启用，将不再接收山石云瞻威胁情报中心中最新的热点威胁情报。

- 列表中指定威胁情报部分，基本信息展示如下内容：

选项	说明
相关威胁事件数量	显示与该威胁情报相关的威胁事件数量。点击对应的数字，跳转至威胁事件列表页面，列表将显示与该威胁情报的CVE编号相匹配的威胁事件。
相关弱点数量	显示与该威胁情报相关的弱点数量。点击对应的数字，跳转至弱点列表页面，列表将显示与该威胁情报的CVE编号相匹配的弱点。
CNNVD编号	显示威胁情报的CNNVD ID及链接。点击链接地址，将打开国家信息安全漏洞库中对应的该漏洞的详情网页。
CVE编号	显示威胁情报的CVE ID及链接。点击链接地址，将打开CVE详情网页。
更新时间	显示威胁情报的更新时间。

- 点击“忽略”按钮，忽略接收到的该条热点威胁情报，忽略后将不能对其创建工单。
- 点击“创建工单”按钮，在打开的页面中新建工单，对威胁情报进行响应，并且通知到指定处理人实施人工处理。

- 在列表中点击任意一条威胁情报名称，打开详情页面，查看威胁情报的介绍、详情、处置建议、关联信息、受影响系统等内容。



威胁情报库

用户可以通过智源平台威胁情报库从云端获取预定义的威胁情报。目前，系统提供的威胁情报库包括山石域名情报库（DNS类）、山石恶意代码情报库（恶意代码类）、山石IP情报库（IP类）、山石URL情报库（URL类）、山石弱点情报库（弱点类）、入侵检测特征库（入侵检测类）和地理库。

威胁情报库升级

威胁情报库升级支持在线升级和离线升级两种方式，用户可根据自身的网络环境进行选择。

在线升级

当设备与互联网相连，能访问到山石网科的威胁情报库升级服务器时，建议用户采用在线升级的方式进行升级。各个威胁情报库的在线升级操作相同，请参考以下步骤：

1. 选择“情报中心 > 威胁情报”，选择任一威胁情报库的标签页。
2. 在线升级支持手动升级和定时升级两种方式。
    - 手动升级：点击“立即升级”按钮，立即升级威胁情报库。
    - 定时升级：点击开启按钮，然后配置升级计划。可以设置“每日”或“每周”的一个固定的时间点进行升级。
3. 升级服务器设置：设备提供两个默认威胁情报库更新服务器，输入update1.hillstonenet.com或update2.hillstonenet.com。

离线升级

当设备无法连接到互联网时，用户可以提前下载威胁情报库文件，然后复制在本地计算机再进行离线升级。下载时，请访问网站：https://update1.hillstonenet.com和https://update2.hillstonenet.com。各个威胁情报库的离线升级操作相同，请参考以下步骤：

1. 点击“选择文件”按钮，在本地计算机选择离线升级的威胁情报库文件（支持.sig格式）。
2. 选择文件后，点击“立即升级”按钮，系统开始上传威胁情报库文件并开始升级。

自定义威胁情报管理

用户可对威胁情报进行自定义配置，即添加自定义白名单情报和黑名单情报。

白名单

白名单包括全局白名单、DNS类白名单和文件类白名单。

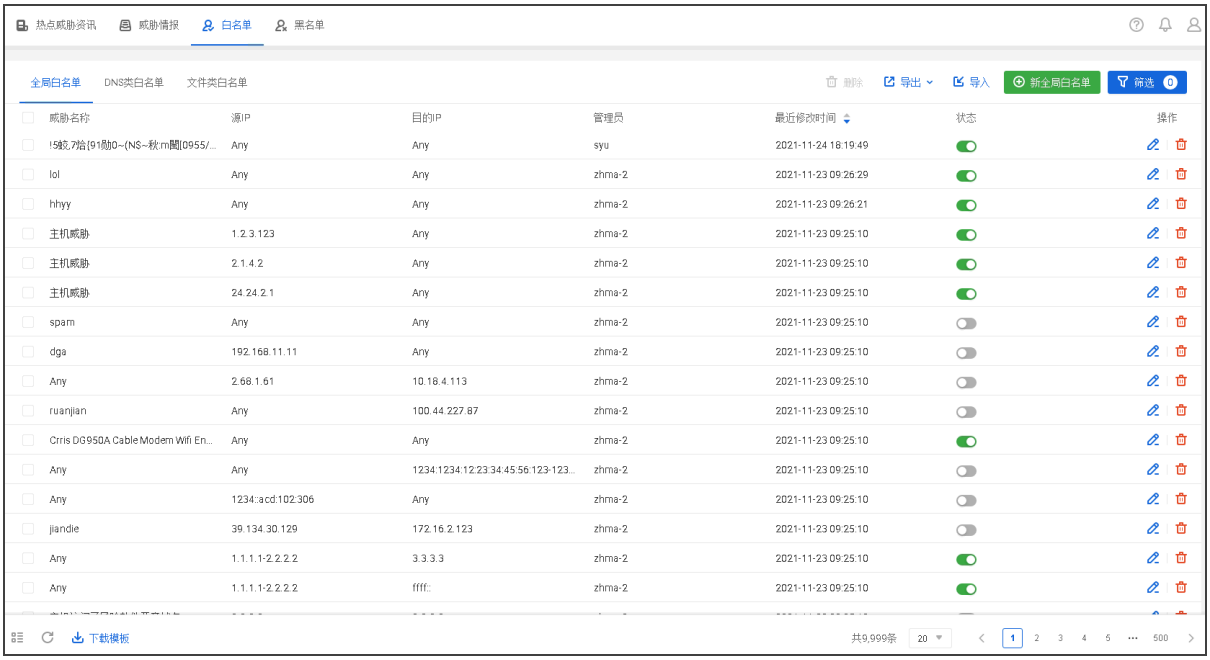
全局白名单

全局白名单包含威胁事件的威胁名称、源IP、目的IP，匹配全局白名单条件的事件产生时，系统将不会检测为威胁事件，从而降低威胁事件的误报率。系统支持通过以下三种方式添加全局白名单：

- 添加已检测到的威胁事件：在威胁事件列表（威胁分析>事件）中，直接将已检测出的威胁事件加入到全局白名单。
- 手动添加：通过自定义源IP、目的IP 以及威胁名称，添加自定义全局白名单条目。
- 导入全局白名单：通过导入全局白名单文件来批量添加全局白名单。

查看全局白名单

选择“情报中心>白名单”，然后选择“全局白名单”页签，进入全局白名单页面。



- 点击上方

按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的白名单信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置” 按钮，删除已经添加的筛选条件。
- 白名单列表的默认排序规则是按照“最近修改时间”进行降序。点击表头中“最近修改时间”后的按钮，可将白名单列表进行重新排序：
  - 点击对应按钮后，当按钮显示为时，将白名单列表按照“最近修改时间”进行降序排列。
  - 点击对应按钮后，当按钮显示为时，将白名单列表按照“最近修改时间”进行升序排列。
  - 当“最近修改时间”后的按钮同时显示为时，将白名单列表进行随机排列。
- 点击列表中的“状态”列的启用按钮启用或禁用指定全局白名单条目。
- 点击列表中的按钮，打开<编辑白名单>页面，
- 点击列表中的按钮，在弹出的对话框中点击“确认”，删除所选条目。如需批量删除全局白名单，勾选多个全局白名单前的复选框或者勾选“威胁名称”前复选框进行全选，然后点击页面右上角的“删除”按钮。
- 点击列表中的“导出”按钮，导出全局白名单，将全局白名单信息从智源平台导出到本地。
- 点击列表中的“导入”按钮，导入全局白名单，将全局白名单文件从本地导入到智源平台。
- 点击“新全局白名单”按钮，手动添加全局白名单条目。
- 点击页面左下角按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角按钮，刷新全局白名单列表。
- 点击页面左下角“下载模板”按钮，下载全局白名单的模板，查看并使用标准的全局白名单文件格式。

手动添加全局白名单

手动添加威胁事件至全局白名单，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“全局白名单”页签，进入全局白名单页面。
2. 点击页面右上角的“新全局白名单”按钮，打开<新全局白名单>页面。



选项	说明
源IP	指定全局白名单条目的源IP地址。若不填写，则默认为Any。请按照以下步骤操作： 1. 点击下拉菜单，选择“IP地址”或“IP地址段”。 2. 点击IPv4或IPv6的单选按钮，指定源IP地址的类型。 3. 在文本框中输入源IP地址或起始IP和结束IP。
目的IP	指定全局白名单条目的目的IP地址。若不填写，则为Any。请按照以下步骤操作：

选项	说明
	1. 点击下拉菜单，选择“IP地址”或“IP地址段”。 2. 点击IPv4或IPv6的单选按钮，指定目的IP地址的类型。 3. 在文本框中输入目的IP地址或起始IP和结束IP。
威胁名称	指定全局白名单条目的威胁名称。默认为Any。支持指定为系统已有的威胁名称（威胁引擎和攻击链引擎中包含的威胁规则）以及自定义威胁名称两种方式。 • 指定为系统已有的威胁名称：点击下拉菜单，直接选择系统中已有的威胁名称；或者在文本框中输入威胁名称关键词，下拉菜单中将展示威胁名称搜索结果，在搜索结果中选择所需的威胁名称。 • 自定义威胁名称：在文本框中直接输入自定义的威胁名称。

3. 点击“确定”，完成配置。

注意: 用户至少选择源IP、目的IP以及威胁名称中的一项进行配置。

下载全局白名单模板

用户可下载模板文件，查看并使用标准的全局白名单文件格式。

下载全局白名单的模板文件，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“全局白名单”页签，进入全局白名单页面。
2. 点击页面左下角“下载模板”按钮，开始下载格式为.xls的模板文件，文件名为“用户名-whitelist-global-template-下载时间”。

####全局白名单文件模板(带*号为必填字段，ip不为空时ip段及ip协议族不能为空，请不要留空白行，导入前请删除示例数据)									
威胁名称	起始源ip	终止源ip	源ip是否为ip段(是/否)	源ip协议族(ipv4/ipv6)	起始目的ip	终止目的ip	目的ip是否为ip段(是/否)	目的ip协议族(ipv4/ipv6)	白名单状态(是/否)*
any	1.1.1.1	2.2.2.2	是	ipv4	3.3.3.3		否	ipv4	是
any	aaaa::	ffff::	是	ipv6	ffff::		否	ipv6	是

根据全局白名单模板，填写如下配置项。

选项	说明
威胁名称	填写威胁事件的名称，不超过512字符。
起始源IP	填写源IP地址，或源IP段的起始地址。
终止源IP	填写源IP段的终止地址。
源IP是否为IP段	填写“是/否”。若源IP不为空时，须填写此项。
源IP协议簇	填写“IPv4/IPv6”。若源IP不为空时，须填写此项。
起始目的IP	填写目的IP地址，或目的IP段的起始地址。
终止目的IP	填写目的IP段的终止地址。
目的IP是否为IP段	填写“是/否”。若目的IP不为空时，须填写此项。
目的IP协议簇	填写“IPv4/IPv6”。若目的IP不为空时，须填写此项。
白名单状态	指定是否启用该条白名单，填写“是/否”。此项为必填项。



注意:

- 在列表中填写全局白名单时，须从上到下依次填写，不可留空白行。
- 威胁名称、源IP和目的IP不能同时为空，为空的字段默认为“Any”。
- 系统最多存储10000条全局白名单信息，因此导入文件中的全局白名单与系统中已存在的全局白名单数量之和须小于等于10000。

导出全局白名单

用户可以将全局白名单从智源平台导出到本地，并且可选择导出全部白名单或只导出选中的部分白名单。

从智源平台导出全局白名单到本地，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“全局白名单”页签，进入全局白名单页面。
2. 点击“导出”按钮，选择“导出全部”或“导出选中项”，开始下载格式为.xls的导出文件，文件名为“用户名-whitelist-global-下载时间”。

注意:

- 选择“导出全部”选项时，将根据当前的筛选条件，导出相应的全局白名单。
- 如智源平台页面中白名单条目参数为“Any”，则导出的文件中的相应参数为空。

导入全局白名单

用户可以将.csv、.xls、.xlsx格式的全局白名单文件从本地导入到智源平台。导入前，建议下载模板文件，并在模板文件中填写白名单信息。

将全局白名单从本地导入智源平台，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“全局白名单”页签，进入全局白名单页面。
2. 点击页面右上角的“导入”按钮，打开<导入全局白名单>页面。



3. 点击“下载模板”，查看并使用全局白名单模板，具体配置请参阅下载全局白名单模板部分。
4. 点击“选择文件”，选择需导入的文件。支持上传.csv、.xls、.xlsx格式的文件。
5. 点击“上传”按钮。
   - 若文件通过系统校验，则弹出导入进度条，完成导入。
   - 若文件未通过系统校验，则显示“导入失败”及错误信息。

DNS类白名单

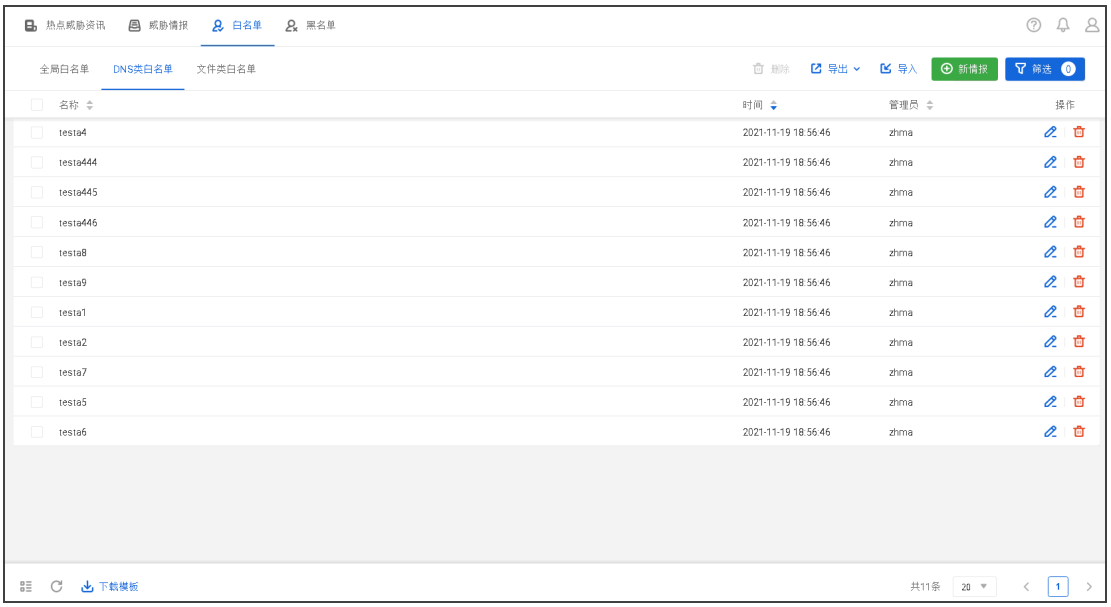
DNS类白名单中的DNS域名将不会被检出为威胁事件，可以通过标记威胁事件、手动添加或导入DNS类白名单三种方式将DNS域名添加至DNS类白名单。

通过以下威胁引擎检测出的威胁事件被标记为误报且将相关域名加入DNS类白名单时，被添加的域名将显示在DNS类白名单列表中：

- 挖矿类威胁引擎中“挖矿通信行为”威胁规则；
- DNS类威胁引擎中除“可疑的DNS隧道行为”和“DNS协议滥用”之外的所有威胁规则；
- 威胁情报类威胁引擎中以“恶意域名”结尾的所有威胁规则。

查看DNS类白名单

选择“情报中心>白名单”，然后选择“DNS类白名单”，进入DNS类白名单页面。



- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的白名单信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 白名单列表的默认排序规则是按照“时间”进行降序。点击表头中“名称”、“时间”或“管理员”后的 按钮，可将白名单列表进行重新排序：
  - 点击对应按钮后，当按钮显示为 时，将白名单列表按照“名称”、“时间”或“管理员”进行降序排列。

    - 点击对应按钮后，当按钮显示为  时，将白名单列表按照“名称”、“时间”或“管理员”进行升序排列。
    - 当“名称”、“时间”和“管理员”后的按钮同时显示为  时，将白名单列表进行随机排列。
- 点击列表中的  按钮，打开<编辑白名单>页面，对所选域名进行编辑。
- 点击列表中的  按钮，在弹出的对话框中点击“确认”，删除所选域名。如需批量删除域名，勾选多个域名条目或者勾选“名称“列复选框进行全选，然后点击页面右上角的“删除”按钮。
- 点击列表中的“导出”按钮，导出DNS类白名单，将DNS类白名单信息从智源平台导出到本地。
- 点击列表中的“导入”按钮，导入DNS类白名单，将DNS类白名单文件从本地导入到智源平台。
- 点击“新情报”按钮，手动添加DNS域名至DNS类白名单。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新DNS类白名单列表。
- 点击页面左下角“下载模板”按钮，下载DNS类白名单的模板，查看并使用标准的DNS类白名单文件格式。

手动添加新域名至DNS类白名单

手动添加DNS域名至DNS类白名单，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“DNS类白名单”标签页，进入DNS类白名单页面。
2. 点击页面右上角的“新情报”按钮。
3. 在打开的<新DNS类白名单>页面中，在“名称”后面的文本框中输入域名。
4. 点击“确定”，完成配置。

下载DNS类白名单模板

用户可下载模板文件，查看并使用标准的DNS类白名单文件格式。

下载DNS类白名单的模板文件，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“DNS类白名单”页签，进入DNS类白名单页面。
2. 点击页面左下角“下载模板”按钮，开始下载格式为.xls的模板文件，文件名为“用户名-whitelist-dns-template-下载时间”。

####DNS类白名单文件模板(带*号为必填字段，请不要留空白行，导入前请删除示例数据)									
域名*									
www									

3. 填写域名。域名每段不超过63字符，完整域名不超过255字符，域名中不能包含特殊字符。此项为必填项。



注意:

- 在列表中填写DNS类白名单时，须从上到下依次填写，不可留空白行。
- 系统最多存储10000条DNS类白名单信息，因此导入文件中的DNS类白名单与系统中已存在的DNS类白名单数量之和须小于等于10000。

导出DNS类白名单

用户可以将DNS类白名单从智源平台导出到本地，并且可选择导出全部白名单或只导出选中的部分白名单。

从智源平台导出DNS类白名单到本地，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“DNS类白名单”页签，进入DNS类白名单页面。
2. 点击“导出”按钮，选择“导出全部”或“导出选中项”，开始下载格式为.xls的导出文件，文件名为“用户名-whitelist-dns-下载时间”。



注意: 选择“导出全部”选项时，将根据当前的筛选条件，导出相应的DNS类白名单。

导入DNS类白名单

用户可以将.csv、.xls、.xlsx格式的DNS类白名单文件从本地导入到智源平台。导入前，建议下载模板文件，并在模板文件中填写白名单信息。

将DNS类白名单信息从本地导入智源平台，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“DNS类白名单”页签，进入DNS类白名单页面。
2. 点击页面右上角的“导入”按钮，打开<导入DNS类白名单>页面。



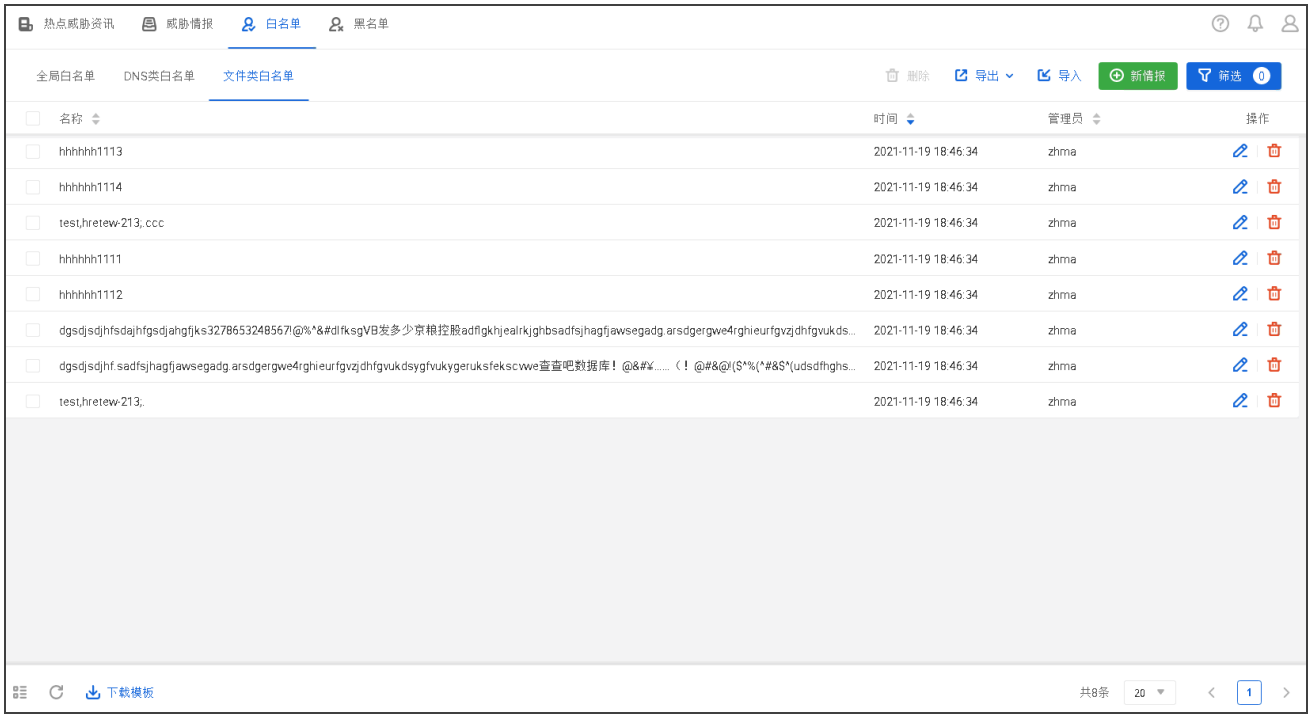
3. 点击“下载模板”，查看并使用DNS类白名单模板，具体配置请参阅下载DNS类白名单模板部分。
4. 点击“选择文件”，选择需导入的文件。支持上传.csv、.xls、.xlsx格式的文件。
5. 点击“上传”按钮。
   - 若文件通过系统校验，则弹出导入进度条，完成导入。
   - 若文件未通过系统校验，则显示“导入失败”及错误信息。

文件类白名单

当使用某些常用应用程序上传或下载文件时，下载文件的后缀名会被临时改变，因此可能会出现文件类检测的误报问题。用户可以通过将可能会产生误报的应用程序添加至文件类白名单，从而减少文件类检测的误报问题。

查看文件类白名单

选择“情报中心>白名单”，然后选择“文件类白名单”，进入文件类白名单页面。



- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的白名单信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 白名单列表的默认排序规则是按照“时间”进行降序。点击表头中“名称”、“时间”或“管理员”后的 按钮，可将白名单列表进行重新排序：
  - 点击对应按钮后，当按钮显示为 时，将白名单列表按照“名称”、“时间”或“管理员”进行降序排列。
  - 点击对应按钮后，当按钮显示为 时，将白名单列表按照“名称”、“时间”或“管理员”进行升序排列。
  - 当“名称”、“时间”和“管理员”后的按钮同时显示为 时，将白名单列表进行随机排列。
- 点击列表中的 按钮，打开<编辑文件类白名单>页面，对所选文件类白名单进行编辑。

- 点击列表中的  按钮，在弹出的对话框中点击“确认”，删除所选条目。如需批量删除文件类白名单，勾选多个文件类白名单或者勾选“名称“列复选框进行全选，然后点击页面右上角的“删除”按钮。
- 点击列表中的“导出”按钮，导出文件类白名单，将文件类白名单信息从智源平台导出到本地。
- 点击列表中的“导入”按钮，导入文件类白名单，将文件类白名单文件从本地导入到智源平台。
- 点击“新情报”按钮，添加文件类白名单条目。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新文件类白名单列表。
- 点击页面左下角“下载模板”按钮，下载文件类白名单的模板，查看并使用标准的文件类白名单文件格式。

添加文件类白名单

手动添加应用程序名称相应关键字至文件类白名单，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“文件类白名单”标签页，进入文件类白名单页面。
2. 点击页面右上角的“新情报”按钮。
3. 在打开的<新文件类白名单>页面中，在“名称”后面的文本框中输入应用程序名称相应关键字，例如“QQ”。
4. 点击“确定”，完成配置。

下载文件类白名单模板

用户可下载模板文件，查看并使用标准的文件类白名单文件格式。

下载文件类白名单的模板文件，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“文件类白名单”页签，进入文件类白名单页面。

2. 点击页面左下角“下载模板”按钮，开始下载格式为.xls的模板文件，文件名为“用户名-whitelist-file-template-下载时间”。

####文件类白名单文件模板(带*号为必填字段，请不要留空白行，导入前请删除示例数据)									
文件名*									
test									

3. 填写URL关键字或文件名，不超过255字符。名称中不能包含如下特殊字符：“\/:*?"<>|”。此项为必填项。

注意:

- 在列表中填写文件类白名单时，须从上到下依次填写，不可留空白行。
- 系统最多存储10000条文件类白名单信息，因此导入文件中的文件类白名单与系统中已存在的文件类白名单数量之和须小于等于10000。

导出文件类白名单

用户可以将文件类白名单从智源平台导出到本地，并且可选择导出全部白名单或只导出选中的部分白名单。

从智源平台导出文件类白名单到本地，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“文件类白名单”页签，进入文件类白名单页面。
2. 点击“导出”按钮，选择“导出全部”或“导出选中项”，开始下载格式为.xls的导出文件，文件名为“用户名-whitelist-file-下载时间”。

注意: 选择“导出全部”选项时，将根据当前的筛选条件，导出相应的DNS类白名单。

导入文件类白名单

用户可以将.csv、.xls、.xlsx格式的文件类白名单文件从本地导入到智源平台。导入前，建议下载模板文件，并在模板文件中填写白名单信息。

将文件类白名单信息从本地导入智源平台，请按照以下步骤进行操作：

1. 选择“情报中心>白名单”，然后选择“文件类白名单”页签，进入文件类白名单页面。
2. 点击页面右上角的“导入”按钮，打开<导入文件类白名单>页面。



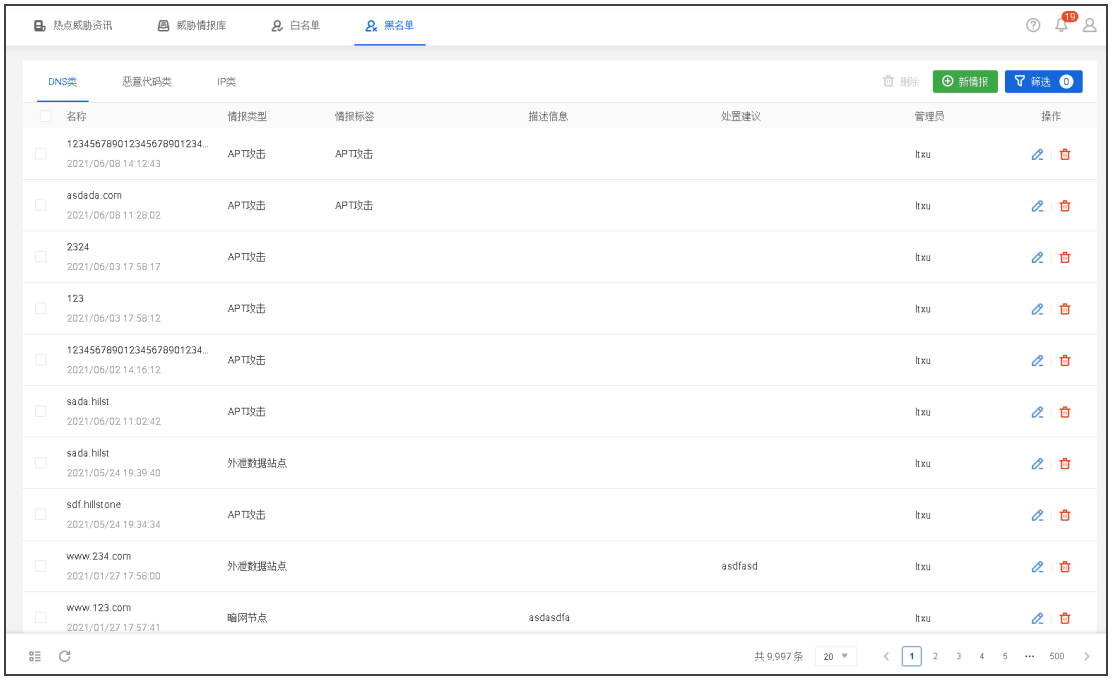
3. 点击“下载模板”，查看并使用全局白名单模板，具体配置请参阅下载文件类白名单模板部分。
4. 点击“选择文件”，选择需导入的文件。支持上传.csv、.xls、.xlsx格式的文件。
5. 点击“上传”按钮。
   - 若文件通过系统校验，则弹出导入进度条，完成导入。
   - 若文件未通过系统校验，则显示“导入失败”及错误信息。

黑名单

黑名单中的DNS域名、恶意软件名或IP地址将会根据对应的威胁规则被检出为对应的威胁事件。用户可手动添加DNS类、恶意代码类和IP类黑名单情报。

查看黑名单

选择“情报中心>黑名单”，进入黑名单页面。



- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的黑名单信息。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击列表中的 按钮，打开<编辑黑名单>页面，对所选情报进行编辑。
- 点击列表中的 按钮，在弹出的对话框中点击“确认”，删除所选情报。如需批量删除情报，勾选多个黑名单情报条目或者勾选“名称“列复选框进行全选，然后点击页面右上角的“删除”按钮。
- 点击“新情报”按钮，手动添加情报至黑名单。

添加新情报至黑名单

手动添加黑名单情报（以DNS类为例），请按照如以下步骤进行操作：

1. 选择“情报中心>黑名单”，然后选择“DNS类”标签页。

2. 点击右上角“新情报”按钮。



在打开的<新DNS类黑名单>页面中（以DNS类为例），填写如下配置项。

选项	说明
名称（必填项）	指定该DNS类情报的域名。
情报类型（必填项）	指定该情报的类型。
情报标签	指定该情报的标签。仅支持选择所属情报类型对应的标签。
描述信息	指定该情报的描述信息。
处置建议	指定针对该情报触发的威胁事件的处置建议。

3. 点击“确定”按钮完成配置。

第9章 资产管理

内网资产是指保障公司运行和获取收益的关键内网IT资产，包括各种服务器及终端。由于内网资产在一个公司运营中占据的重要性，最有可能成为攻击者的首选目标。因此，内网资产需要较高的关注度和防御优先级。配置内网资产后，可以配合态势监控功能，对内网资产进行全方面的监测，并且可以在"威胁" 在第115页页面查看内网资产的统计详情以及相关联的威胁。

资产管理部分包含如下内容：

- "资产管理" 在第338页：提供了各类型资产的总览以及详细的资产列表信息，介绍如何配置资产信息。用户可根据需求创建、编辑或删除资产，同时支持导入/导出资产。
- "资产探测" 在第359页：介绍如何配置资产探测任务相关信息。用户可以根据需求配置任务的类型以及扫描范围，同时可以在扫描结果列表中对资产进行入库、忽略、更新等操作。
- "区域管理" 在第363页：介绍如何配置区域相关信息。用户可根据需求将内网资产划分到不同区域中。
- "业务管理" 在第369页：介绍如何配置业务相关信息。用户可根据实际情况将运行相同业务的服务器配置到指定业务名称下。
- "待入库资产" 在第375页：介绍如何配置待入库资产相关信息。用户可根据实际情况入库或忽略相关的资产。
- "待更新资产" 在第381页：介绍如何配置待更新资产的相关信息。用户可根据实际情况更新或删除相关的资产。

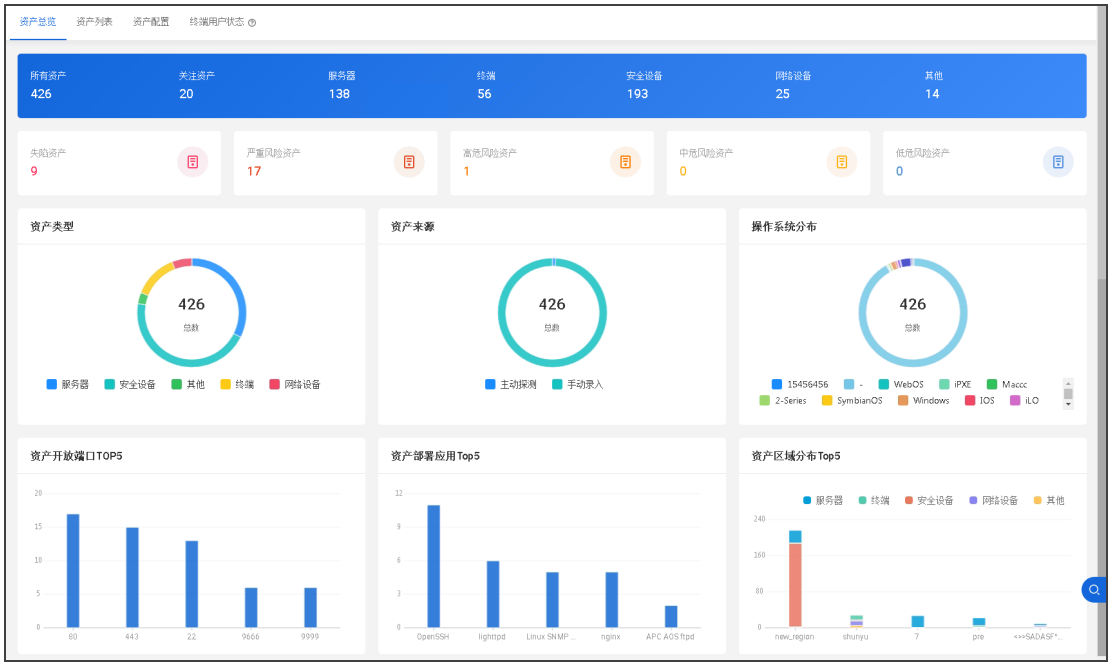
资产管理

资产管理页面提供了各类型资产的总览以及详细的资产列表信息，帮助用户整体把握系统中的资产情况与精准查看每一条资产的详细信息。用户可以根据需要创建新的资产，或者对已有的资产进行编辑和删除操作。另外，支持查看或下线当前的终端在线用户。

资产总览

资产总览页面统计并展示了资产的相关概览。例如，各种类型的资产数量和占比、资产来源的比例、操作系统的分布、开放端口Top5、部署应用Top5以及区域分布Top5。

点击“资产管理”，进入资产管理页面。在<资产总览>标签页，展示资产的相关概览。



- 点击页面上方各种类型资产的数字，跳转至<资产列表>标签页，页面上将展示指定类型的资产的信息。例如：点击“关注资产”下的数字，页面跳转至<资产列表>标签页，并展示了全部资产中设为重点关注的资产。
- 点击页面上方各种风险等级的资产对应的数字，跳转至<全部资产风险>页面，系统自动将“30天”作为筛选条件展示对应风险等级的资产信息。例如：点击“失陷资产”下的数字，页面跳转至<全部资产风险>页面，并展示30天内全部疑似失陷的资产。
    - 资产类型、资产来源以及操作系统分布圆环图直观展示了不同资产的分布占比情况。

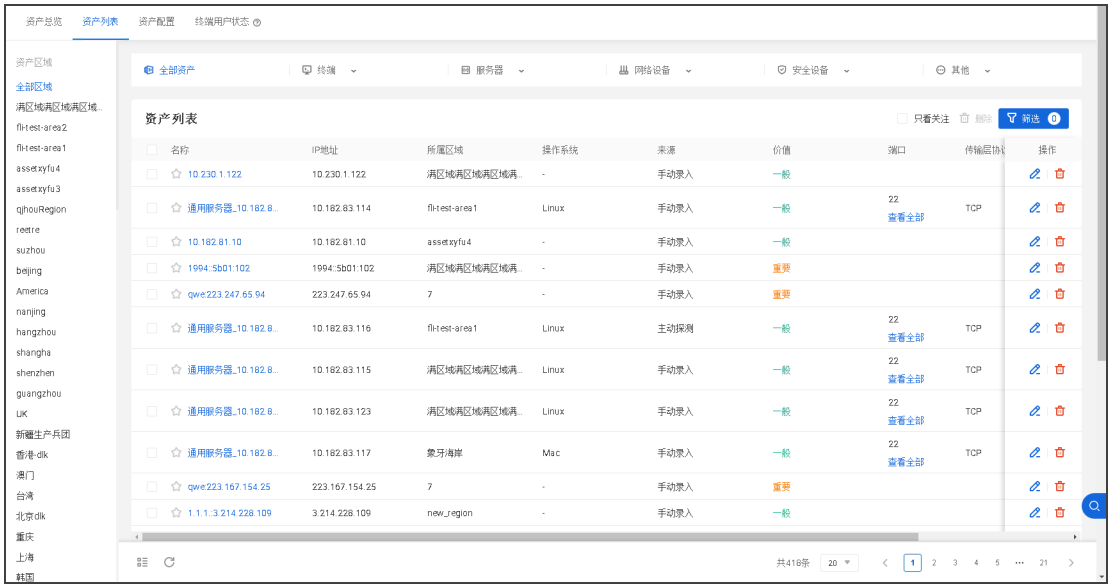
- 圆环中间显示资产总数。
- 点击图例，图例变灰，取消所选资产在圆环图中的统计展示。
- 鼠标悬停在圆环图各部分，显示对应资产的数量或操作系统的数量和占比。
- 点击圆环图指定部分，跳转至<资产列表>标签页，并展示指定条件的资产的信息。

- 资产开放端口Top5、资产部署应用Top5以及资产区域分布Top5柱状图直观地展示了资产中排名前5的常见端口、部署应用以及关联资产数量排名前5的区域。
  - 鼠标悬停在柱状图各部分，显示对应开放端口和部署应用的数量，以及区域中各种类型的资产的具体数量。
  - 点击图例，图例变灰，取消所选资产在柱状图中的统计展示。
  - 点击柱状图指定部分，跳转至<资产列表>标签页，并展示指定条件的资产的信息或指定区域特定类型的资产信息。

资产列表

资产列表页面展示了系统中的全部资产的详细信息，同时支持通过筛选资产区域、资产类型等来查看特定资产的信息。资产列表中最多支持展示500000条资产信息。

点击“资产管理”，进入资产管理页面。在<资产列表>标签页，展示内网中所有手动录入（包括创建、导入和被动发现）和主动探测到的资产信息。



- 点击页面左侧“资产区域”列中的区域，页面右侧资产列表将展示出指定区域的资产信息。资产区域支持多选，再次点击可取消选中。
- 点击页面右侧上方的资产类型，资产列表将展示出指定类型的资产信息。当选中“终端”、“服务器”、“网络设备”、“安全设备”或“其他”类型的资产时，可以进一步选择其中的子类来筛选资产。
- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击列表中具体资产前的 按钮，可将该资产设为重点关注资产，同时需要在下拉框中选择告警通知人。将资产设为关注后，系统将自动生成对应告警规则。此资产上若发生用户设置的关注威胁事件或严重、高危事件时，都会向管理员发出告警。最多支持关注100条资产。
- 勾选列表上方“只看关注”前的复选框，列表中将展示所有被设为重点关注的资产。
- 点击资产“名称”链接，查看所选资产的详细信息。
- 点击资产列表中“操作”列的  按钮，打开“编辑资产”页面，编辑所选资产。
- 点击资产列表中“操作”列的  按钮，在弹出的对话框中点击“确定”，删除所选资产。如需批量删除资产，勾选多个资产条目或者勾选“名称“列复选框进行全选，然后点击页面右上角的“删除”按钮。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新资产列表。

查看资产详情

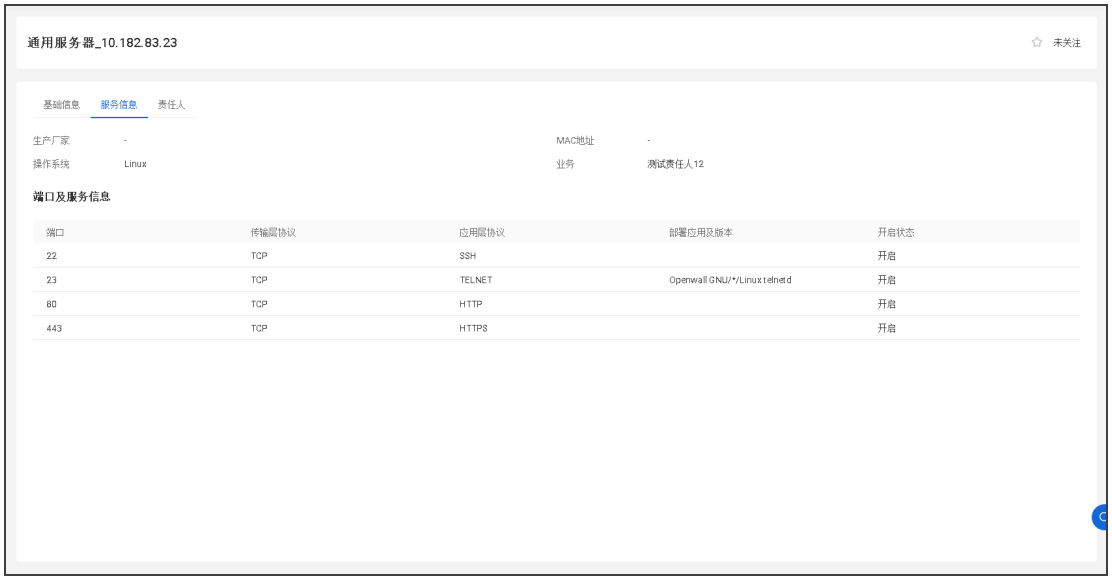
在详细信息页面可以查看所选资产的基础信息、服务信息和责任人信息。页面上方显示资产的名称和关注状态，若要更改资产的关注状态，请在资产列表页面操作。

点击<基础信息>标签页，查看资产的基础信息。



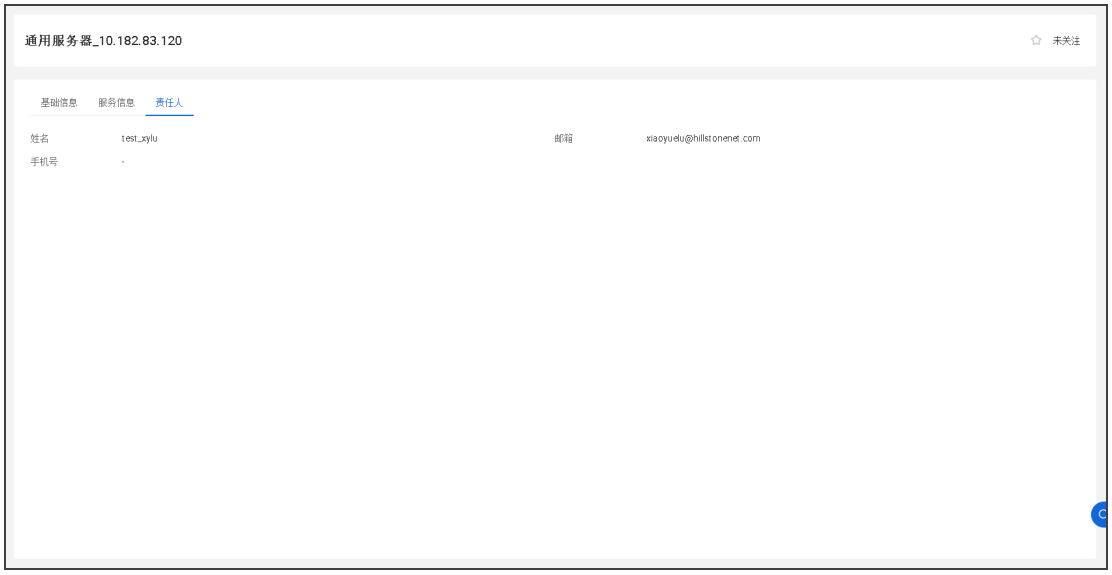
信息	说明
资产名称	查看资产的名称。用户可以在编辑资产的<基础信息>页面修改资产名称。
资产类型	查看资产的类型，结构为“大类-子类”。用户可以在编辑资产的<基础信息>页面修改资产的类型。
资产IP	查看资产的IP地址。
价值	查看资产的价值，包括“重要”和“一般”两种。用户可以在编辑资产的<基础信息>页面修改资产的价值。
所属区域	查看资产所属的区域。用户可以在编辑资产的<基础信息>页面修改资产的区域。
来源	查看资产的来源，包括“手动录入”和“主动探测”两种。 • 手动录入方式通过创建资产、导入资产以及流量识别实现。 • 主动探测方式通过创建资产探测任务实现。
首次发现时间	查看系统第一次发现发现该资产的时间。
更新时间	查看系统最近一次更新该资产的时间。

点击<服务信息>标签页，查看资产的服务信息。



信息	说明
生产厂家	查看资产的生产厂家。用户可以在编辑资产的<基础信息>页面修改资产的生产厂家。
MAC地址	查看资产的MAC地址。用户可以在编辑资产的<基础信息>页面修改资产的MAC地址。
操作系统	查看资产的操作系统。用户可以在编辑资产的<基础信息>页面修改资产的操作系统。
业务	查看资产的业务。用户可以在编辑资产的<基础信息>页面修改资产的业务。
端口及服务信息	查看资产的端口号、传输层协议、应用层协议、部署应用及版本、开启状态。端口和服务信息的获取方式有3种，包括创建资产时配置，主动探测任务自动探测以及解析弱点报告获得。

点击<责任人>标签页，查看资产的责任人信息。



信息	说明
姓名	查看责任人的姓名。用户可以在编辑资产页面修改责任人信息。
邮箱	查看责任人的邮箱。用户可以在编辑资产页面修改责任人信息。
手机号	查看责任人的手机号。用户可以在编辑资产页面修改责任人信息。

编辑资产

编辑资产，请按照以下步骤进行操作：

1. 点击“资产管理 > 资产列表”，进入<资产列表>标签页。
2. 点击资产列表中资产条目后的按钮，在<编辑资产>弹出框中，配置资产的信息。

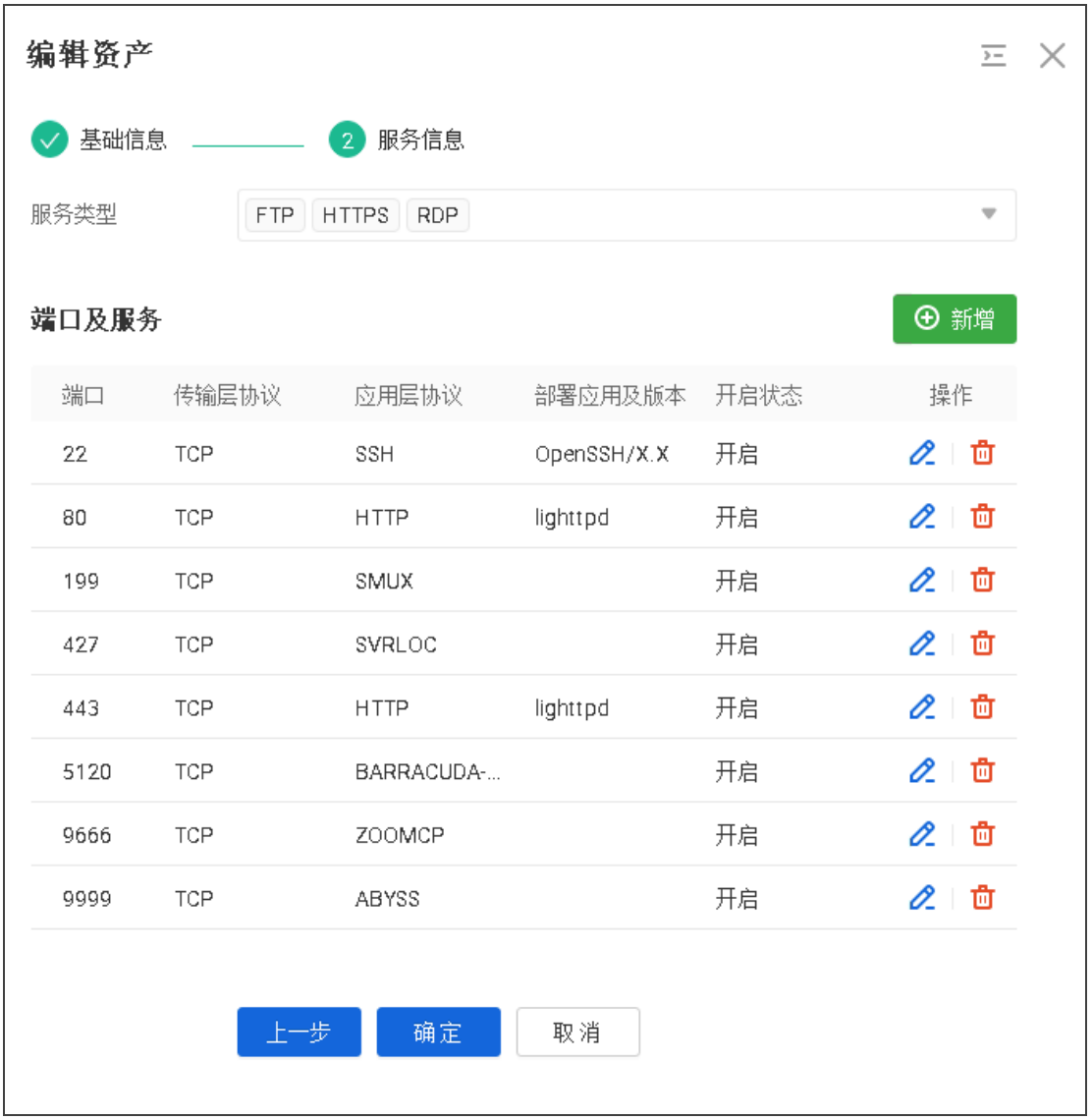


在<基础信息>页面，填写相关配置信息。

选项	说明
名称（必填）	输入资产的名称。
资产类型（必	在下拉框中选择资产的类型。资产大类包括“终端”、“服

选项	说明
填）	务器”、“网络设备”、“安全设备”以及“其他”，点击大类后的 > 按钮，进一步配置资产所属的子类。
所属区域（必填）	在下拉列表中选择资产所属的区域。关于区域，参见新建区域。
业务	在下拉列表中勾选业务名称的复选框，指定资产运行的业务，可多选。关于业务，参见新建业务。
操作系统	输入或在下拉列表中选择资产的操作系统。
MAC地址	输入资产的MAC地址。
生产厂家	输入资产的生产厂家。
价值（必填）	指定资产的价值，包括重要和一般。
责任人	点击下拉菜单打开联系人列表，选择资产的责任人，仅可单选。 • 在搜索框中输入指定的联系人名称，点击 搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“责任人”选项中已选择的资产责任人。
描述	输入资产的描述信息。

3. 点击“下一步”，进入<服务信息>页面。



在<服务信息>页面，填写相关配置。

服务类型	在下拉列表中勾选服务协议的复选框，指定资产的服务类型，可多选。
端口及服务	用户可以新增、编辑和删除资产的端口及服务。 • 点击 新增 按钮，弹出<新增端口及服务>配置框。 • 端口：配置资产端口号，不可重复。

- 传输层协议：输入该端口上的传输层协议。
- 应用层协议：输入该端口上的应用层协议。
- 开启状态：点击“启用”按钮，启用该端口。
- 部署应用：输入端口上的应用，
  如：OpenSSH。
- 部署应用版本：输入该应用的版本号，
  如：1.1。

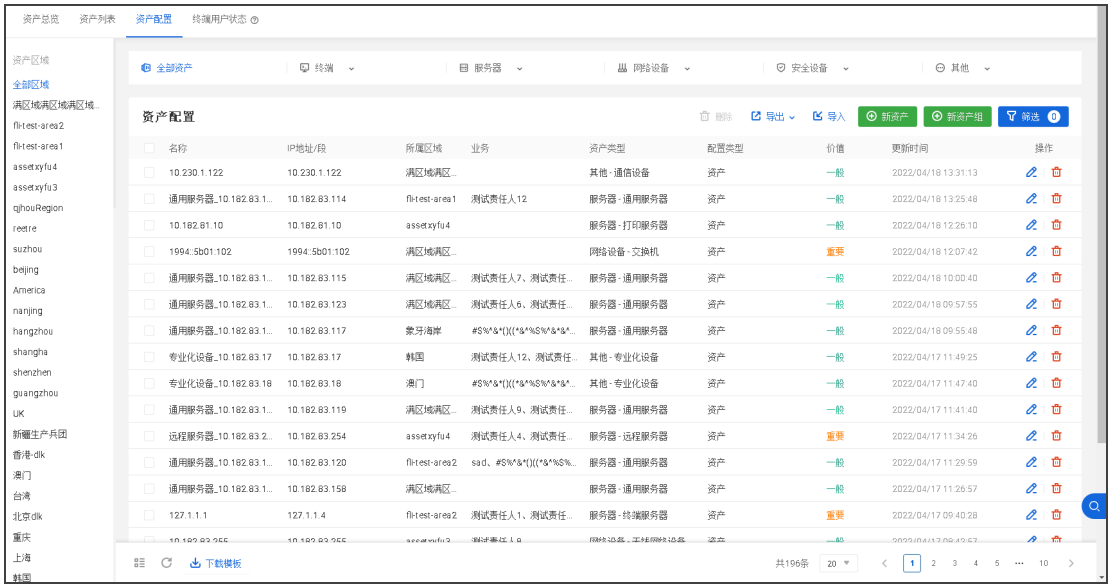
- 点击列表条目后的按钮，编辑该条目。
- 点击列表条目后的按钮，删除该条目。

4. 点击“确定”，完成配置。

资产配置

系统支持创建或从本地导入资产、资产组，同时支持将系统中的资产、资产组导出到本地。

点击“资产管理”，进入资产管理页面。在<资产配置>标签页，展示内网中所有创建和导入的资产信息，同时支持创建和导入新的资产。



- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产或资产组。圆圈中的数字表示已配置筛选条件的个数，点击 “重置” 按钮，删除已经添加的筛选条件。
- 点击资产列表中资产或资产组条目后的  按钮，打开 “编辑资产” 或 “编辑资产组” 页面，编辑所选资产或资产组。可参考新建资产或新建资产组。
- 点击资产列表中资产或资产组条目后的  按钮，删除所选资产或资产组。如需批量删除资产或资产组，勾选多个资产条目，点击 “删除” 按钮。
- 点击 “导出” 按钮，导出资产或资产组，将资产或资产组信息从智源平台导出到本地。
- 点击 “导入” 按钮，导入资产或资产组，将资产或资产组信息从本地导入到智源平台。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新资产列表。
- 点击 “下载模板”，下载模板文件，查看标准的资产或资产组信息文件格式。

新建资产

新建资产，请按照以下步骤进行操作：

1. 点击“资产管理”。

2. 在<资产配置>标签页，点击“新资产”按钮，打开<新资产>页面。



在<新资产>页面，填写相关配置信息。

选项	说明
名称（必填项）	输入资产的名称。

选项	说明
IP地址（必填项）	指定资产IP地址类型，IPv4或者IPv6，然后输入资产的IP地址。
资产类型（必填项）	在下拉框中选择资产的类型。资产大类包括“终端”、“服务器”、“网络设备”、“安全设备”以及“其他”，点击大类后的 > 按钮，进一步配置资产所属的子类。
所属区域（必填项）	在下拉列表中选择资产所属的区域。关于区域，参见新建区域。
业务	在下拉列表中勾选业务名称的复选框，指定资产运行的业务，可多选。关于业务，参见新建业务。
操作系统	输入或在下拉列表中选择资产的操作系统。
服务类型	在下拉列表中勾选服务协议的复选框，指定资产的服务类型，可多选。
价值（必填）	指定资产的价值，包括重要和一般。
责任人	点击下拉菜单打开联系人列表，选择资产的责任人，仅可单选。 • 在搜索框中输入指定的联系人名称，点击 搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“责任人”选项中已选择的资产责任人。
描述	输入资产的描述信息。

3. 点击“确定”按钮完成配置。

新建资产组

新建资产组，请按照以下步骤进行操作：

1. 点击“资产管理”。

2. 在<资产配置>标签页，点击“新资产组”按钮，打开<新资产组>页面。



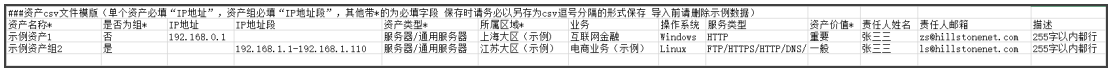
在<新资产组>页面，填写相关配置信息。

选项	说明
名称（必填项）	输入资产组的名称。
IP地址段（必填项）	指定资产IP地址类型，IPv4或者IPv6，然后再输入资产组的起始IP地址和终止IP地址，并点击“添加”按钮，添加IP地址段。内网中IP地址在指定IP地址段的资产会被识别出来，并显示在资产列表中。 用户可在同一资产组下添加多个IP地址段。
资产类型（必填项）	在下拉列表中选择资产组的类型。资产大类包括“终端”、“服务器”、“网络设备”、“安全设备”以及“其他”，点击大类后的 > 按钮，进一步配置资产组所属的子类。
所属区域（必填项）	在下拉列表中选择资产所属的区域。关于区域，参见新建区域。
业务	在下拉列表中勾选业务名称的复选框，指定资产组运行的业务，可多选。关于业务，参见新建业务。
服务类型	在下拉列表中勾选服务协议的复选框，指定资产组的服务类型，可多选。
价值（必填）	指定资产组的价值，包括重要和一般。
责任人	点击下拉菜单打开联系人列表，选择资产组的责任人，仅可单选。 • 在搜索框中输入指定的联系人名称，点击 搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“责任人”选项中已选择的资产组责任人。
描述	输入资产组的描述信息。

3. 点击“确定”按钮完成配置。

下载模板

用户可下载模板文件，查看标准的资产或资产组信息文件格式。模板内容如下图所示：



###资产csv文件模版（单个资产必填“IP地址”，资产组必填“IP地址段”，其他带*的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）											
资产名称*	是否为组*	IP地址	IP地址段	资产类型*	所属区域*	业务	操作系统	服务类型	资产价值*	责任人姓名	责任人邮箱	描述
示例资产1	否	192.168.0.1		服务器/通用服务器	上海大区（示例）	互联网金融	Windows	HTTP	重要	张三三	zs@hillstonenet.com	255字以内部行
示例资产组2	是		192.168.1.1-192.168.1.110	服务器/通用服务器	江苏大区（示例）	电商业务（示例）	Linux	FTP/HTTPS/HTTP/DNS/	一般	张三三	ls@hillstonenet.com	255字以内部行

下载资产或资产组信息的模板文件，请按照以下步骤进行操作：

1. 选择“资产管理 > 资产配置”，进入资产配置页面。
2. 点击“下载模板”按钮，开始下载格式为.csv的模板文件，文件名为“用户名-asset-all-下载时间”。

导出资产或资产组

用户可以将资产或资产组信息从智源平台导出到本地，并且可选择导出全部资产或资产组信息或只导出选中的部分资产或资产组信息。

从智源平台导出资产或资产组信息到本地，请按照以下步骤进行操作：

1. 选择“资产管理 > 资产配置”，进入资产配置页面。
2. 点击“导出”按钮，选择“导出全部”、“导出选中项”、“导出资产配置”或“导出资产组配置”，开始下载格式为.csv的导出文件。选择“导出全部”或“导出选中项”时，文件名为“用户名-asset-all-导出时间”；选择“导出资产配置”时，文件名为“用户名-asset-single-导出时间”；选择“导出资产组配置”时，文件名为“用户名-asset-group-导出时间”。

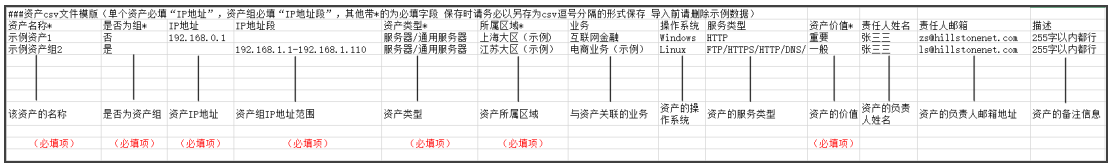
注意:

- 系统最多支持同时导出2000条资产或资产组信息。
- 如导出的资产或资产组信息中存在空白项，则导出文件中的相应参数也为空。

导入资产或资产组

用户可以将资产或资产组信息从本地导入到智源平台。导入前，建议下载模板文件，并在模板文件中填写资产或资产组信息。

下图为.csv格式的资产或资产组信息文件及参数实例：



###资产csv文件模版（单个资产必填“IP地址”，资产组必填“IP地址段”，其他带*的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）												
资产名称*	是否为组*	IP地址	IP地址段	资产类型*	所属区域*	业务	操作系统	服务类型	资产价值*	责任人姓名	责任人邮箱	描述
示例资产1	否	192.168.0.1		服务器/通用服务器	上海大区（示例）	互联网金融	Windows	HTTP	重要	张三三	zs@hillstonenet.com	255字以内都行
示例资产组2	是		192.168.1.1-192.168.1.110	服务器/通用服务器	江苏大区（示例）	电商业务（示例）	Linux	FTP/HTTPS/HTTP/DNS/	一般	张三三	ls@hillstonenet.com	255字以内都行
该资产的名称	是否为资产组	资产IP地址	资产组IP地址范围	资产类型	资产所属区域	与资产关联的业务	资产的操作系统	资产的服务类型	资产的价值	资产的负责人姓名	资产的负责人邮箱地址	资产的备注信息
（必填项）	（必填项）	（必填项）	（必填项）	（必填项）	（必填项）				（必填项）			

注意:

- 在导入资产或资产组信息前，请参照上图并将资产或资产组信息按照格式要求填写。
- 填写资产或资产组信息时，用户须注意以下事项：
  - “资产/组名称”为必填项，互相不能重复。
  - “资产类型”为必填项，且需包括大类和子类，格式为“大类/子类”。大类包含“终端”、“服务器”、“网络设备”、“安全设备”以及“其他”。
    - “终端”中的子类包括：打印机、网络电话、游戏主机、媒体设备、掌上电脑、手机、数据存储设备、网络摄像头、终端。
    - “服务器”中的子类包括：通用服务器、终端服务器、打印服务器、代理服务器、远程服务器。
    - “网络设备”中的子类包括：交换机、宽带路由器、无线网络设备、负载均衡设备、路由器、网络电话适配器、电话交换机、集线器、网桥。
    - “安全设备”中的子类包括：防火墙、安全设备。
    - “其他”中的子类包括：通信设备、专业化设备、电源设备、其他设备。



- “资产价值”须填写“重要”或“一般”。
- “所属区域”为必填项，须填写系统中已存在的区域名称。
- “业务”须填写系统中已存在的业务名称。或者可先导入相关的业务信息文件，将相关业务导入成功后，再导入资产配置信息文件。可填写多个业务（以“/”隔开），如“业务1/业务2”。
- “服务类型”的可填写项包括：FTP/DNS/HTTP/HTTPS/IMAP4/RDP/LDAP/POP3/SMTP/HTTP-Proxy/SNMP/MySQL/MSSQL。可填写多项（以“/”隔开），如“FTP/DNS”。
- 若当前系统已存在导入文件中的责任人，则可只填写“责任人姓名”而不填写对应的“责任人邮箱”。

- 填写资产信息时，用户须注意以下事项：
  - “是否为组”为必填项，须填写“否”。
  - “IP地址”为必填项，须符合IP地址规范，且不与其他IP地址重复。
  - 不填写“IP地址段”。
  - “操作系统”列可输入操作系统名称，取值范围为1-32字符。
- 填写资产组信息时，用户须注意以下事项：
  - “是否为组”为必填项，须填写“是”。
  - “IP地址段”为必填项，须符合IP地址规范（起始地址-结束地址）。可以包含其他资产的IP地址，但不可与其他资产组的IP地址段重复。用户可填写多个IP地址段（以“;”隔开），如“156.23.42.1-156.23.42.10;172.36.78.1-172.36.78.10”。在同一个资产组下，不能同时填写IPv4地址段和IPv6地址段。
  - 不填写“IP地址”。

将资产或资产组信息从本地导入智源平台，请按照以下步骤进行操作：

1. 选择“资产管理 > 资产配置”，进入资产配置页面。
2. 点击“导入”按钮，打开<导入资产>页面。



3. 点击“选择文件”，选择所需导入的文件。选择后若需更换文件，点击“取消”按钮。
4. 点击“上传”按钮，系统会对导入的文件进行校验。
5. （可选）校验和上传过程中可以点击“取消”按钮取消本次导入。

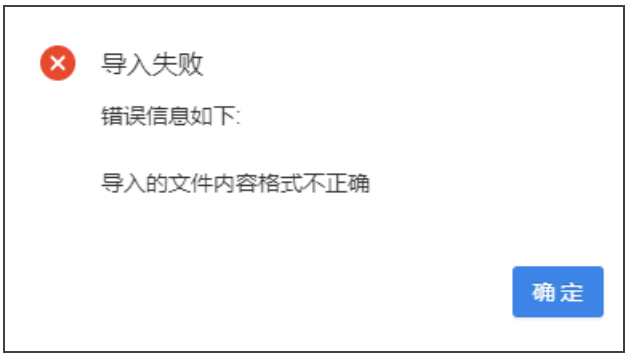
注意:

- 系统最多存储2000条资产或资产组信息，因此导入文件中的资产或资产组信息与系统中已存在的资产或资产组信息数量之和须小于等于2000。
- 若需要同时导入相关联的业务信息，则应首先导入业务信息，后导入资产或资产组信息。
- 若需要同时导入相关联的区域信息，则应首先导入区域信息，后导入资产或资产组信息。
- 若当前系统里不存在导入文件中的责任人，则系统自动创建新责任人。

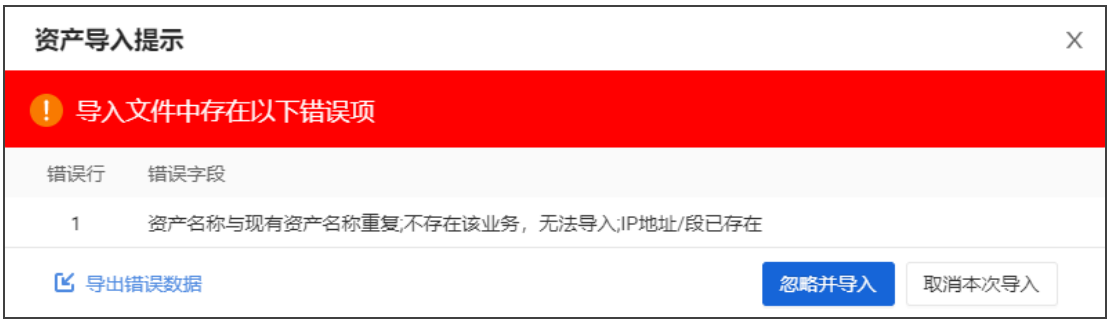
错误提示

系统的校验过程首先校验文件本身的合法性，再校验文件中配置项的合法性。若文件通过系统校验，则完成导入。若文件未通过系统校验，包含以下两种可能出现的情况：

1. 若文件不合法，则无法导入该文件，例如：文件中条目加上已有条目超过限制、文件内容格式不正确等。此时弹出“导入失败”框，并提示失败的原因。



2. 若文件合法，但文件中配置项不合法，例如：名称重复。此时弹出“资产导入提示”框，展示错误出现的行数以及错误的字段。

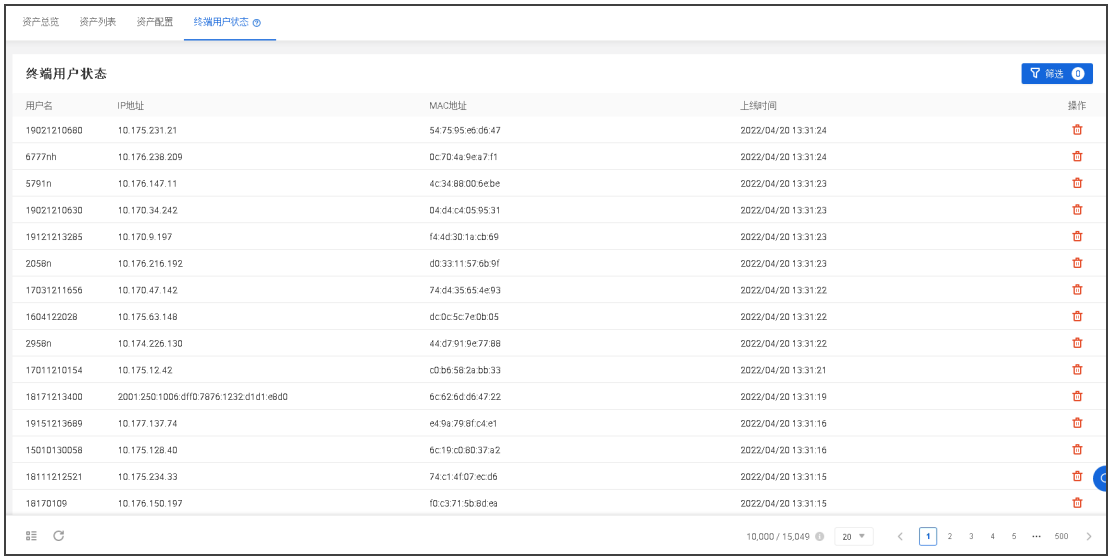


- 点击“导出错误数据”，导出格式为.csv的文件到本地，文件名为“用户名-asset-errorlist-导出时间”。
- 点击“忽略并导入”，忽略对该错误条目的导入操作，并导入其他符合条件的资产条目。
- 点击“取消本次导入”，取消对全部资产的导入操作。

终端用户状态

智源平台支持与第三方认证服务器（深澜认证计费系统Srun4000）对接，从接收的计费开始或更新报文中提取接入网络的终端使用的用户名、IP、MAC地址和上线时间，展示在用户状态标签页下的在线用户表中。当智源平台收到认证计费结束报文后，对应的用户条目从在线用户表中删除。

点击“资产管理”，进入资产管理页面。在<终端用户状态>标签页，可以查看当前在线的用户信息。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的在线用户。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击在线用户列表中用户条目后的 按钮，删除所选用户的在线记录，手动将所选用户的在线状态标记为下线。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新在线用户展示列表。

注意: 若同一用户同时使用不同的终端设备接入网络，则分别展示多条该用户的用户信息。

资产探测

设备支持主动探测资产以提升添加资产的效率，通过配置资产探测任务主动发现新资产或识别老资产的更新信息，用户可以在任务的结果列表中查看探测到的资产信息，并执行入库、忽略、更新等操作。任务探测到的资产信息以及对资产的相关操作均会同步到<待入库资产>或<待更新资产>页面。同时，用户在<待入库资产>或<待更新资产>页面对相关资产的操作，也会同步到探测任务的结果列表。

点击“资产管理 > 资产探测”，进入资产探测页面。



- 资产探测任务列表默认按照任务状态升序排列。点击表头中“启动时间”或“任务状态”后的 按钮，可将资产探测任务进行重新排序：
  - 点击对应按钮后，当按钮显示为 时，将资产探测任务按照降序排列。
  - 点击对应按钮后，当按钮显示为 时，将资产探测任务按照升序排列。
  - 当按钮显示为 时，资产探测任务恢复默认排列。
- “启动时间”列展示了最近一次启动该资产探测任务的时间。
- “任务类型”列展示了该任务的类型，包括“资产探测”和“资产更新”。资产探测任务根据扫描网段进行资产识别探测；资产更新任务只针对已入库的老资产进行二次探测，识别更新信息。
- “任务状态”列展示了该任务目前的状态，包括等待中、运行中、失败、已结束和已取消5种状态类型。
- “新发现资产”列展示了资产探测任务探测到的新资产数量，点击数字跳转至探测结果界面。在结果页面可查看该任务相关的新发现资产、已忽略资产以及入库记录，同时可以对新发现的资产进行入库或忽略操作。具体配置方法可参考“待入库资产 > 主动探测”。

- “待更新资产”列展示了资产探测任务探测到的待更新的老资产数量，点击数字跳转至探测结果界面。在结果页面可查看该任务相关的待更新资产和更新记录，同时可以对待更新的资产进行更新或删除操作。具体配置方法可参考“待更新资产”。
- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的任务。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击 新任务 按钮，创建新的资产探测任务，具体配置可参考新建资产探测任务。
- 点击“操作”列的按钮，编辑指定的资产探测任务，具体配置可参考新建资产探测任务。编辑任务配置后，将清空其当前的扫描结果列表，并且重新启动该任务。“待入库资产”和“待更新资产”页面的总列表中的同步结果不会被删除。
- 点击“操作”列的按钮，删除指定的资产探测任务。如需批量删除任务，勾选多个任务条目，点击“删除”按钮。“待入库资产”和“待更新资产”页面的总列表中的同步结果不会被删除。
- 点击“操作”列的 按钮，启动资产探测任务，“操作”列按钮变为 ，此时点击 按钮，可取消该任务。已取消的任务，将保留当前已经探测到的结果。
  同一时间只能执行一项任务，启动多项任务时，只有最开始启动的任务状态为“进行中”，其余任务将处于等待状态。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新资产探测列表。



注意: 若不同探测任务均发现识别到同一IP的资产，在同步到待入库资产和待更新资产总列表中时，最新发现的结果会覆盖之前的结果。

新建资产探测任务

新建资产探测任务，请按照以下步骤进行操作：

1. 点击“资产管理 > 资产探测”，进入<资产探测>页面。

2. 点击页面右上方 新任务 按钮，弹出<新建资产探测任务>对话框。



在<新建资产探测任务>页面，填写相关配置信息。

选项	说明
任务名称（必填项）	输入任务名称。
任务类型（必填项）	选择任务类型为“资产探测”或“资产更新”。默认情况下任务类型为资产探测。 • 当选择“资产探测”时，系统根据扫描网段进行资产识别探测。 • 当选择“资产更新”时，系统只针对已入库的老资产进行二次探测，识别更新信息。
扫描网段（必填）	当任务类型为资产探测时，配置探测任务扫描的网段。可配置为IP/掩码类型或指定IP地址段。仅支持IPv4类型的地址。
应用及版本号	选择探测任务是否扫描资产的应用及版本号。默认情况下

选项	说明
（必填项）	不扫描。 注意：若选择扫描应用及版本号，将会大幅度降低扫描速度。

3. 点击“确定”，完成配置。

区域管理

为了方便管理在不同地区的内网资产，用户可根据需求将内网资产划分到不同区域中。

点击“资产管理 > 区域管理”，打开区域管理页面。



- “区域管理”列表部分展示所有已创建的区域。
- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的区域。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击“导出”按钮，导出区域，将区域信息从智源平台导出到本地。
- 点击“导入”按钮，导入区域，将.csv格式的区域信息文件从本地导入到智源平台。
- 点击区域管理列表中区域条目后的 按钮，打开“编辑区域”页面，编辑所选区域。
- 点击区域管理列表中区域条目后的 按钮，删除所选区域。如需批量删除区域，勾选多个区域条目，点击“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。

- 点击页面左下角 按钮，刷新区域列表。
- 点击“下载模板”，下载模板文件，查看标准的区域信息文件格式。

新建区域

1. 点击“资产管理 > 区域管理”。
2. 在区域管理页面，点击“新区域”按钮，打开<新区域>页面。



在<新区域>页面，填写相关配置信息。

选项	说明
区域名称（必填项）	输入区域的名称。
所在地区（必填项）	在下拉列表中选择区域所在的国家或地区。
责任人	点击下拉菜单打开联系人列表，选择区域的责任人，仅可单选。 • 在搜索框中输入指定的联系人名称，点击搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“责任人”选项中已选择的区域责任人。
重要程度	指定区域的重要程度为重要或一般。
描述	输入区域的描述信息。

3. 点击“确定”按钮完成配置。

下载模板

用户可下载模板文件，查看标准的区域信息文件格式。模板内容如下图所示：

1	###区域csv文件模版（带*号的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）					
2	区域名称*	重要程度*	所在地区*	责任人姓名	责任人邮箱	描述
3	江苏大区（示例）	重要	中国/江苏省/苏州市	张三三	zs@hillstonene	64字以内都行
4	上海大区（示例）	一般	中国/上海市/上海市	李四四	lisi@hillstonen	64字以内都行
5						

下载区域信息的模板文件，请按照以下步骤进行操作：

1. 选择“资产管理>区域管理”，进入区域管理页面。
2. 点击“下载模板”按钮，开始下载格式为.csv的模板文件，文件名为“用户名-asset-region-下载时间”。

导出区域

用户可以将区域信息从智源平台导出到本地，并且可选择导出全部区域信息或只导出选中的部分区域信息。

从智源平台导出区域信息到本地，请按照以下步骤进行操作：

1. 选择“资产管理>区域管理”，进入区域管理页面。
2. 点击“导出”按钮，选择“导出全部”或“导出选中项”，开始下载格式为.csv的导出文件，文件名为“用户名-asset-region-导出时间”。



注意:

- 系统最多支持同时导出200条区域信息。
- 如导出的区域信息中存在空白项，则导出文件中的相应参数也为空。

导入区域

用户可以将.csv格式的区域信息文件从本地导入到智源平台。导入前，建议下载模板文件，并在模板文件中填写区域信息。

下图为.csv格式的区域信息文件及参数实例：

	A	B	C	D	E	F
1	###区域csv文件模版（带*号的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）					
2	区域名称*	重要程度*	所在地区*	责任人姓名	责任人邮箱	描述
3	江苏大区（示例）	重要	中国/江苏省/苏州市	张三三	zs@hillstonene	该区域为重要区域
4						
5						
6						
7						
8	该区域的名称	该区域的重要程度	该区域所在地区	该区域责任人姓名	责任人邮箱	该区域备注信息
9						
10	（必填项）	（必填项）	（必填项）			
11						

注意:

- 在导入区域信息前，请参照上图并将区域信息按照格式要求填写。
- 填写区域信息时，用户须注意以下事项：
  - “区域名称”为必填项，且不能重复。
  - “重要程度”须填写“重要”或“一般”。
  - “所在地区”为必填项，且须按照“国家/省份/城市”的格式填写。
  - 若当前系统已存在导入文件中的责任人，则可只填写“责任人姓名”而不填写对应的“责任人邮箱”。

将区域信息从本地导入智源平台，请按照以下步骤进行操作：

1. 选择“资产管理>区域管理”，进入区域管理页面。
2. 点击“导入”按钮，打开<导入区域>页面。
3. 点击“选择文件”，选择所需导入的文件。选择后若需更换文件，点击“取消”按钮。
4. 点击“上传”按钮，系统会对导入的文件进行校验。
5. （可选）校验和上传过程中可以点击“取消”按钮取消本次导入。

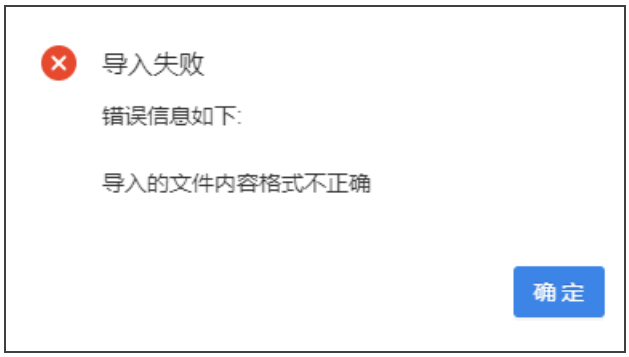
注意:

- 系统最多存储200条区域信息，因此导入文件中的区域信息与系统中已存在的区域信息数量之和须小于等于200。
- 若当前系统里不存在导入文件中的责任人，则系统自动创建新责任人。

错误提示

系统的校验过程首先校验文件本身的合法性，再校验文件中配置项的合法性。若文件通过系统校验，则完成导入。若文件未通过系统校验，包含以下两种可能出现的情况：

1. 若文件不合法，则无法导入该文件，例如：文件中条目加上已有条目超过限制、文件内容格式不正确等。此时弹出“导入失败”框，并提示失败的原因。



2. 若文件合法，但文件中配置项不合法，例如：区域名称重复。此时弹出“资产导入提示”框，展示错误出现的行数以及错误的字段。



- 点击“导出错误数据”，导出格式为.csv的文件到本地，文件名为“用户名-asset-errorlist-导出时间”。
- 点击“忽略并导入”，忽略对该错误条目的导入操作，并导入其他符合条件的区域条目。
- 点击“取消本次导入”，取消对全部区域的导入操作。

业务管理

系统支持配置业务信息，用户可根据实际情况将运行相同业务（为用户提供的服务，如DNS服务、邮件服务等）的服务器配置到指定业务名称下。

点击“资产管理 > 业务管理”，打开业务管理页面。



- “业务管理”列表部分展示所有已创建的业务。
- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的业务。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击“导出”按钮，导出业务，将业务信息从智源平台导出到本地。
- 点击“导入”按钮，导入业务，将业务信息从本地导入到智源平台。
- 点击业务管理列表中业务条目后的 按钮，打开“编辑业务”页面，编辑所选业务。
- 点击业务管理列表中业务条目后的 按钮，删除所选业务。如需批量删除业务，勾选多个业务条目，点击“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新业务列表。
- 点击“下载模板”，下载模板文件，查看标准的业务信息文件格式。

新建业务

新建业务，请按照以下步骤进行操作：

1. 点击“资产管理 > 业务管理”。

2. 在业务管理页面，点击“新业务”按钮，打开<新业务>页面。



在<新业务>页面，填写相关配置信息。

选项	说明
业务名称（必填项）	输入业务的名称。
重要程度	指定业务的重要程度为重要或一般。
责任人	点击下拉菜单打开联系人列表，选择业务的责任人，仅可单选。 • 在搜索框中输入指定的联系人名称，点击搜索指定的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“责任人”选项中已选择的业务责任人。
资产配置	在下拉列表中勾选资产名称的复选框，指定运行该业务的资产。
描述	输入业务的描述信息。

3. 点击“确定”按钮完成配置。

下载模板

用户可下载模板文件，查看标准的业务信息文件格式。模板内容如下图所示：

	A	B	C	D	E	F	G	H
1	###业务csv文件模版（带*号的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）							
2	业务名称*	重要程度*	责任人姓名	责任人邮箱	描述			
3	互联网金融业务（示例）	重要	张三	abc@abc.com	64字以内都行			
4	电商业务（示例）	一般	李四	dfg@dfg.com	64字以内都行			
5								

下载业务信息的模板文件，请按照以下步骤进行操作：

1. 选择“资产管理>业务管理”，进入业务管理页面。
2. 点击“下载模板”按钮，开始下载格式为.csv的模板文件，文件名为“用户名-asset-business-下载时间”。

导出业务

用户可以将业务信息从智源平台导出到本地，并且可选择导出全部业务信息或只导出选中的部分业务信息。

从智源平台导出业务信息到本地，请按照以下步骤进行操作：

1. 选择“资产管理>业务管理”，进入业务管理页面。
2. 点击“导出”按钮，选择“导出全部”或“导出选中项”，开始下载格式为.csv的导出文件，文件名为“用户名-asset-business-导出时间”。



注意:

- 系统最多支持同时导出200条业务信息。
- 如导出的业务信息中存在空白项，则导出文件中的相应参数也为空。

导入业务

用户可以将业务信息从本地导入到智源平台。导入前，建议下载模板文件，并在模板文件中填写业务信息。

下图为.csv格式的业务信息文件及参数实例：

	A	B	C	D	E	F	G	H
1	###业务csv文件模版（带*号的为必填字段 保存时请务必以另存为csv逗号分隔的形式保存 导入前请删除示例数据）							
2	业务名称*	重要程度*	责任人姓名	责任人邮箱	描述			
3	互联网金融业务（示例）	重要	张三	abc@abc.com	64字以内都行			
4	电商业务（示例）	一般	李四	dfg@dfg.com	64字以内都行			
5								
6								
7								
8	该业务的名称	该业务的重要程度	该业务责任人姓名	责任人邮箱	该业务的备注信息			
9								
10	（必填项）	（必填项）						
11								



注意:

- 在导入业务信息前，请参照上图并将业务信息按照格式要求填写。
- 填写业务信息时，用户须注意以下事项：
  - “业务名称”为必填项，且不能重复。
  - “重要程度”须填写“重要”或“一般”。
  - 若当前系统已存在导入文件中的责任人，则可只填写“责任人姓名”而不填写对应的“责任人邮箱”。

将业务信息从本地导入智源平台，请按照以下步骤进行操作：

1. 选择“资产管理>业务管理”，进入业务管理页面。
2. 点击“导入”按钮，打开<导入业务>页面。
3. 点击“选择文件”，选择所需导入的文件。选择后若需更换文件，点击“取消”按钮。
4. 点击“上传”按钮，系统会对导入的文件进行校验。
5. （可选）校验和上传过程中可以点击“取消”按钮取消本次导入。



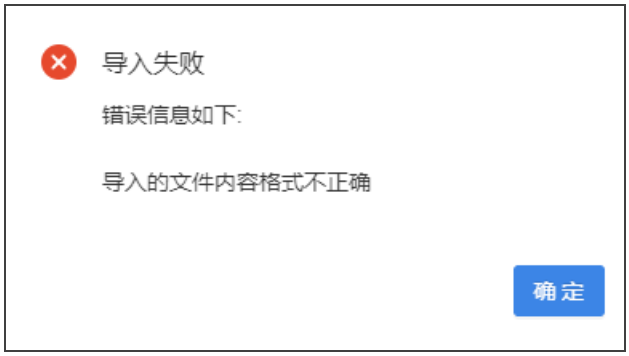
注意:

- 系统最多存储200条业务信息，因此导入文件中的业务信息与系统中已存在的业务信息数量之和须小于等于200。
- 若当前系统里不存在导入文件中的责任人，则系统自动创建新责任人。

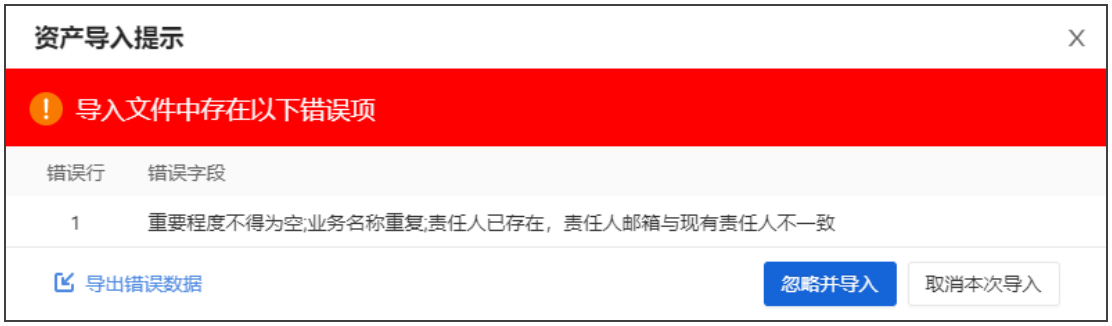
错误提示

系统的校验过程首先校验文件本身的合法性，再校验文件中配置项的合法性。若文件通过系统校验，则完成导入。若文件未通过系统校验，包含以下两种可能出现的情况：

1. 若文件不合法，则无法导入该文件，例如：文件中条目加上已有条目超过限制、文件内容格式不正确等。此时弹出“导入失败”框，并提示失败的原因。



2. 若文件合法，但文件中配置项不合法，例如：业务名称重复。此时弹出“资产导入提示”框，展示错误出现的行数以及错误的字段。



- 点击“导出错误数据”，导出格式为.csv的文件到本地，文件名为“用户名-asset-errorlist-导出时间”。
- 点击“忽略并导入”，忽略对该错误条目的导入操作，并导入其他符合条件的业务条目。
- 点击“取消本次导入”，取消对全部业务的导入操作。

待入库资产

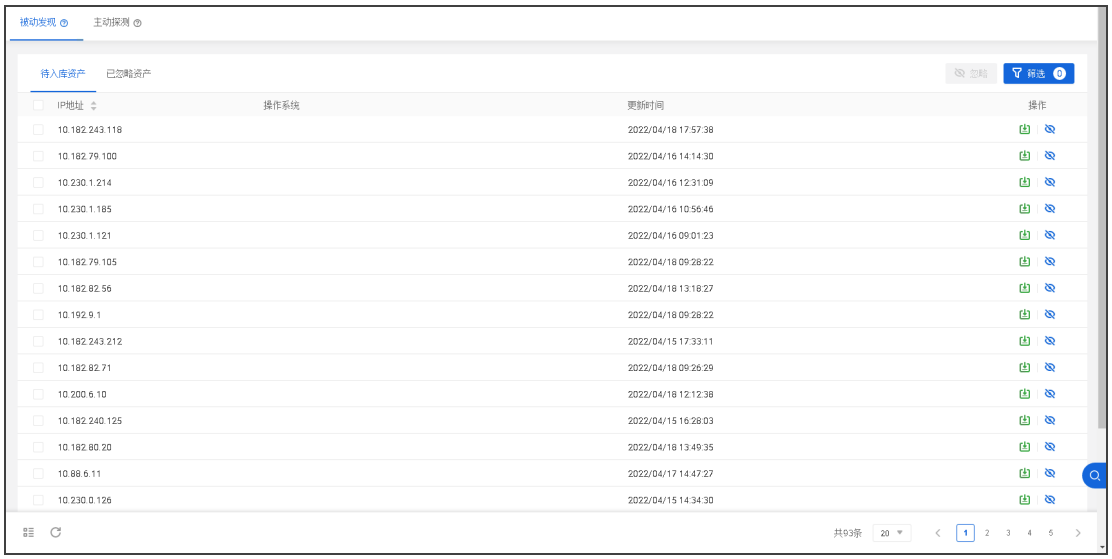
系统聚合所有主动探测任务获得的资产和被动发现的资产，并筛选出未入库的资产展示在列表中。被动发现的资产来自威胁日志、流量日志等。用户可以查看、忽略这些资产，或将有用的资产入库。

被动发现

点击“资产管理 > 待入库资产”，进入待入库资产页面。在<被动发现>标签页，展示待入库和已忽略的被动发现的资产。

待入库资产

在<待入库资产>标签页，展示了所有待入库的被动发现的资产的信息，包括IP地址、操作系统和更新时间。同时，用户可以根据需要处置待入库资产，包括入库和忽略。



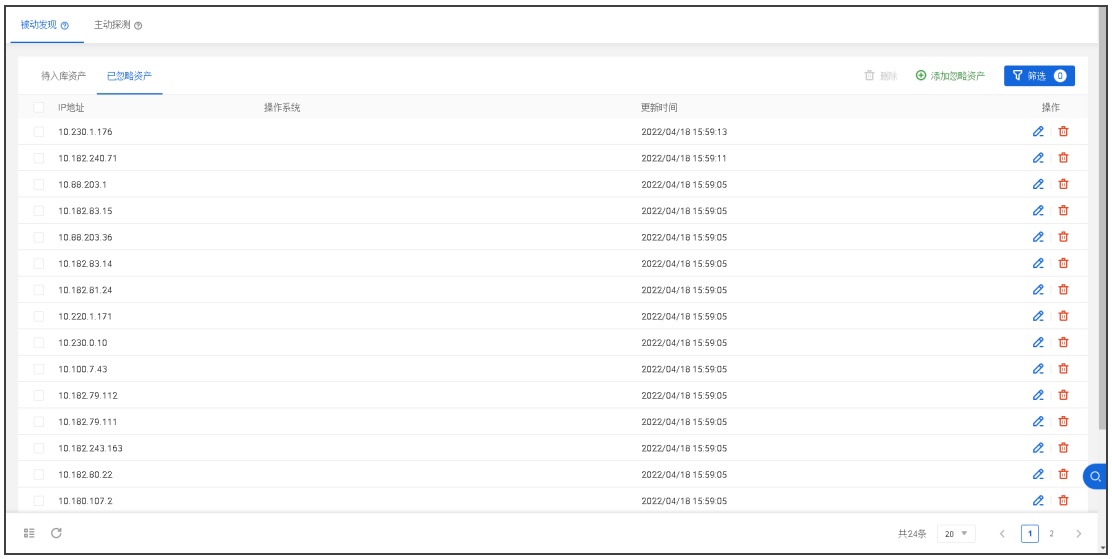
- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。

- 点击待入库资产列表中资产条目后的 按钮，将所选资产入库。具体配置方法可参考编辑资产。

- 点击待入库资产列表中资产条目后的 按钮，弹出“确认忽略所选条目”的确认框，点击“确定”，所选条目将被加入到<已忽略资产>标签页的列表中。点击“取消”则不加入。若忽略多个条目，可在列表中选择需忽略的条目，点击列表右上方的“忽略”按钮。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新待入库资产列表。

已忽略资产

在<已忽略资产>标签页，展示了所有已经忽略的资产的信息。已忽略的资产不会被识别为待入库的被动发现资产，但是，如果已忽略的资产被加入到资产组，将会继续被识别为资产。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击已忽略资产列表中资产条目后的按钮，编辑已忽略资产的IP地址类型、忽略资产网段的起始IP和终止IP以及选择操作系统类型。
- 点击已忽略资产列表中资产条目后的 按钮，将该已忽略资产删除，删除后系统可以继续发现该资产。若删除多个条目，可在列表中选择需忽略的条目，点击列表右上方的“删除”按钮。

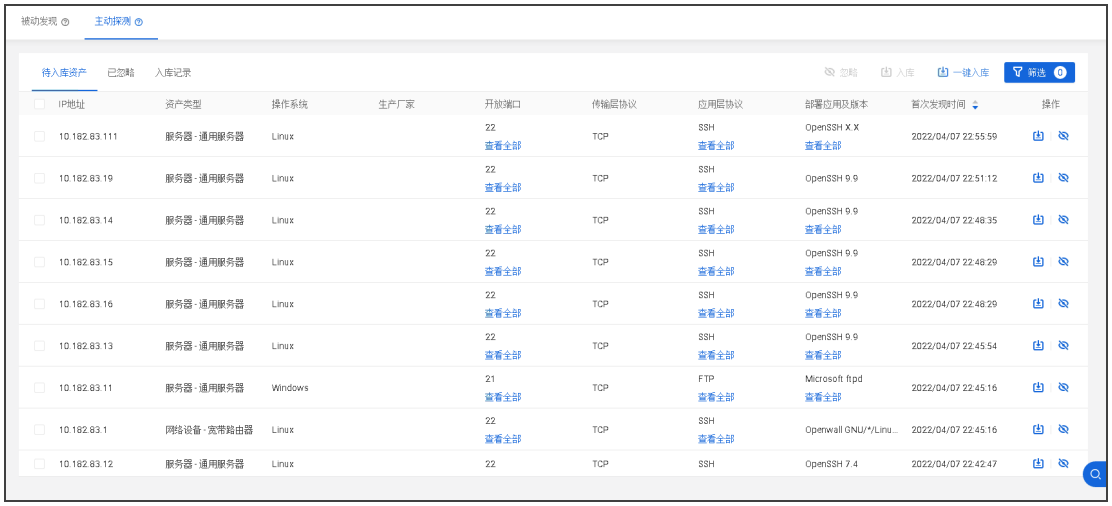
- 点击列表上方 添加忽略资产 按钮，手动添加忽略资产，该资产以后不会被系统发现。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新已忽略资产列表。

主动探测

点击“资产管理 > 待入库资产”，进入待入库资产页面。在<主动探测>标签页，展示待入库和已忽略的主动探测到的资产，以及资产的入库记录。

待入库资产

在<待入库资产>标签页，展示了所有待入库的主动探测到的资产的信息，包括IP地址、操作系统和首次发现时间等。同时，用户可以根据需要处置待入库资产，包括入库和忽略。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击列表中“查看全部”按钮，查看资产全部的端口、应用层协议或部署应用及版本。
- 待入库资产的默认排序规则是按照“首次发现时间”进行降序。点击表头中“首次发现时间”后的 按钮，可将待入库资产进行重新排序：

    - 点击对应按钮后，当按钮显示为  时，将待入库资产按照“首次发现时间”进行降序排列。
    - 点击对应按钮后，当按钮显示为  时，将待入库资产按照“首次发现时间”进行升序排列。
    - 当“首次发现时间”后的按钮显示为  时，将待入库资产进行随机排列。
- 点击待入库资产列表中资产条目后的  按钮，将所选资产入库。具体配置方法可参考编辑资产。若同时入库多条资产，可在列表中选择需要入库的条目，点击列表右上方的“入库”按钮；若要将全部条目都入库，直接点击列表右上方的“一键入库”按钮。同时入库多条资产时，仅需配置资产的命名规则、所属区域、价值和责任人。操作后的结果将同步到资产探测任务的结果列表。
- 点击待入库资产列表中资产条目后的  按钮，弹出“确认忽略所选条目”的确认框，点击“确定”，所选条目将被加入到<已忽略资产>标签页的列表中。点击“取消”则不加入。若忽略多个条目，可在列表中选择需忽略的条目，点击列表右上方的“忽略”按钮。操作后的结果将同步到资产探测任务的结果列表。
- 点击页面左下角  按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角  按钮，刷新待入库资产列表。

已忽略

在<已忽略资产>标签页，展示了所有已经忽略的资产的信息。已忽略的资产不会被系统继续发现，只有当已忽略资产被删除后，系统才能继续识别并发现该资产。

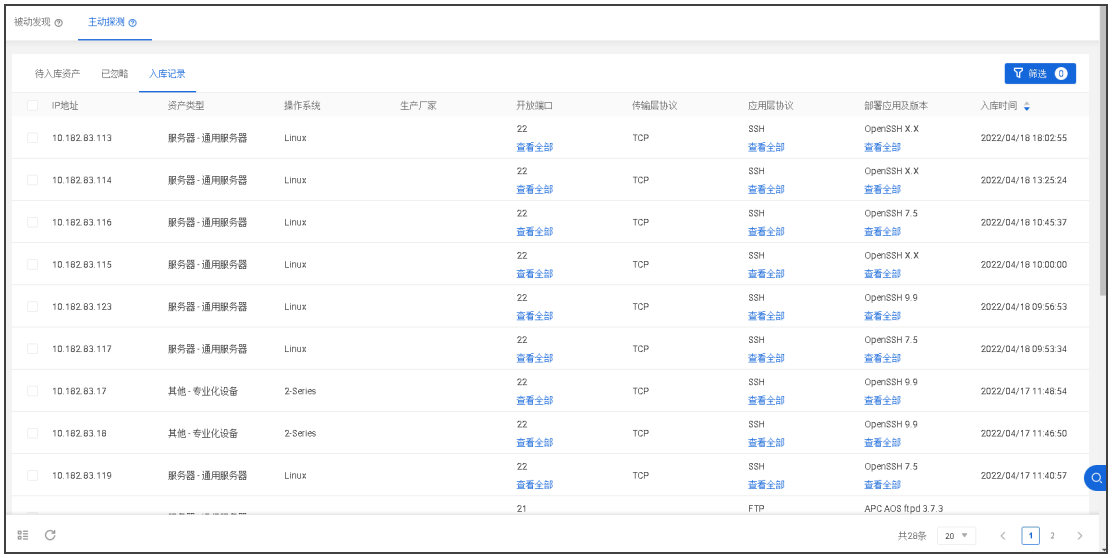
- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。

- 点击已忽略资产列表中资产条目后的 按钮，将该已忽略资产删除，删除后系统可以继续发现该资产。若删除多个条目，可在列表中选择需忽略的条目，点击列表右上方的“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新已忽略资产列表。

入库记录

在<入库记录>标签页，展示了所有入库资产的信息，包括IP地址、操作系统和入库时间等。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击列表中“查看全部”按钮，查看资产全部的端口、应用层协议或部署应用及版本。
- 资产的入库记录的默认排序规则是按照“入库时间”进行降序。点击表头中“入库时间”后的 按钮，可将已入库资产进行重新排序：

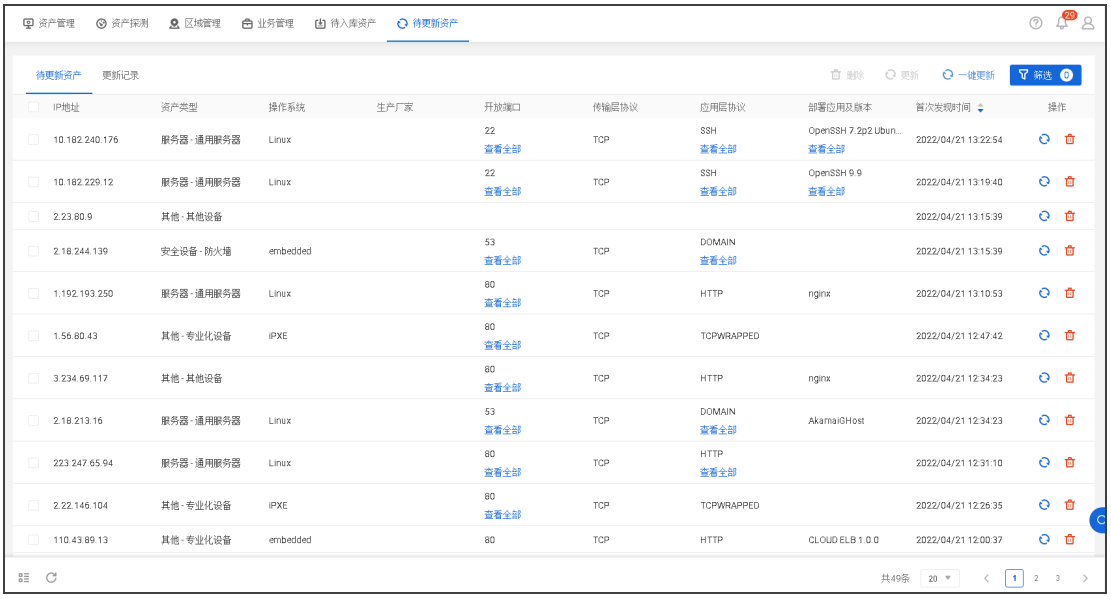
- 点击对应按钮后，当按钮显示为  时，将资产按照“入库时间”进行降序排列。
- 点击对应按钮后，当按钮显示为  时，将资产按照“入库时间”进行升序排列。
- 当“入库时间”后的按钮同时显示为  时，将资产进行随机排列。

待更新资产

资产主动探测任务在探测过程中会识别到已入库的老资产的更新信息，并同步到<待更新资产>页面。待更新资产页面支持查看待更新资产的信息，以及执行更新或删除操作。更新后的资产将会移动到更新记录列表并从待更新资产列表中删除。

待更新资产

点击“资产管理 > 待更新资产”，进入<待更新资产>页面。在“待更新资产”标签页，展示所有待更新资产的相关信息。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击列表中“查看全部”按钮，查看资产全部的端口、应用层协议或部署应用及版本。
- 待更新资产的默认排序规则是按照“首次发现时间”进行降序。点击表头中“首次发现时间”后的 按钮，可将待更新资产进行重新排序：

- 点击对应按钮后，当按钮显示为 时，将待更新资产按照“首次发现时间”进行降序排列。
- 点击对应按钮后，当按钮显示为 时，将待更新资产按照“首次发现时间”进行升序排列。
- 当“首次发现时间”后的按钮显示为 时，将待更新资产进行随机排列。

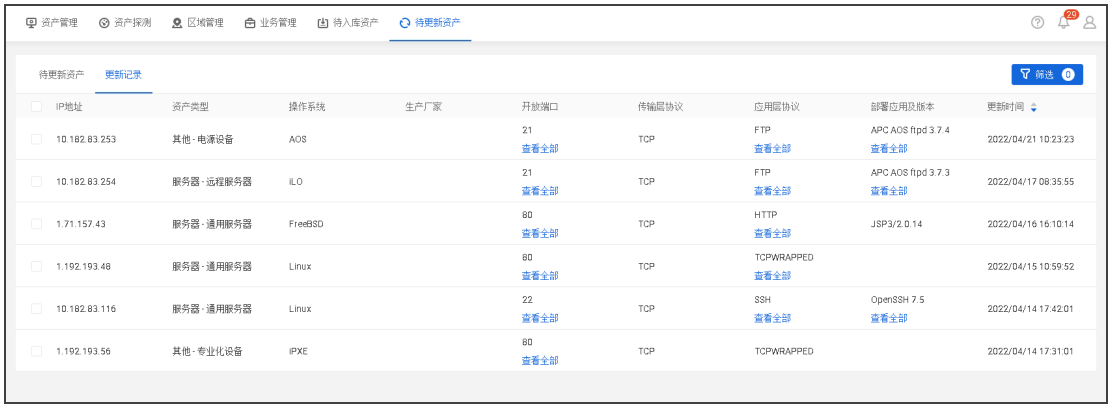
- 点击待更新资产列表中资产条目后的 按钮，更新所选资产。具体配置方法可参考编辑资产。若同时更新多条资产，可在列表中选择需要更新的条目，点击列表右上方的“更新”按钮；若要将全部条目都更新，直接点击列表右上方的“一键更新”按钮。
- 点击待更新资产列表中资产条目后的 按钮，弹出“确认删除所选条目”的确认框，点击“确定”。若删除多个条目，可在列表中选择需删除的条目，点击列表右上方的“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新待入库资产列表。



注意: 更新单个资产时，若该待更新的资产已从资产列表中删除，此时执行更新操作，会将该资产重新添加到资产列表；批量或一键更新资产时，若其中有资产已被删除，将忽略对该资产的更新操作。

更新记录

点击“资产管理 > 待更新资产”，进入<待更新资产>页面。在“更新记录”标签页，展示所有已更新资产的相关信息。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的资产。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击列表中“查看全部”按钮，查看资产全部的端口、应用层协议或部署应用及版本。
- 资产的更新记录的默认排序规则是按照“更新时间”进行降序。点击表头中“更新时间”后的 按钮，可将已更新资产进行重新排序：
  - 点击对应按钮后，当按钮显示为 时，将资产按照“更新时间”进行降序排列。
  - 点击对应按钮后，当按钮显示为 时，将资产按照“更新时间”进行升序排列。
  - 当“更新时间”后的按钮同时显示为 时，将资产进行随机排列。

第10章 引擎管理

引擎管理页面提供多种类型的威胁/攻击链引擎（多个威胁事件类型组成的引擎），当来自于山石网科安全设备、流量探针和用户主机的数据匹配威胁/攻击链引擎时，智源平台将检测到该引擎对应类型的威胁，并在"威胁" 在第115页页面展示相关威胁事件。

引擎管理部分包含如下内容：

- "威胁引擎" 在第385页：介绍如何修改默认威胁引擎或配置威胁关联分析，以检测威胁引擎对应类型的威胁。
- "攻击链引擎" 在第402页：介绍如何修改默认攻击链引擎或配置攻击链关联分析，以检测攻击链引擎对应类型的威胁。

威胁引擎

智源平台提供默认威胁引擎和威胁关联分析。

- 默认威胁引擎：由引擎库提供，包括扫描类、文件类、HTTP检测类、可疑协议类、暴力破解类、DNS类、勒索类、挖矿类、USB行为类、违规访问类和威胁情报类。每个类型的默认威胁引擎都包含一个或多个默认威胁规则，用户可直接使用或编辑后使用默认威胁规则，但不可以删除默认威胁引擎和其包含的规则。
- 威胁关联分析：用来分析智源平台采集到的日志信息。威胁关联分析包括网络威胁日志类关联分析、主机威胁日志类关联分析（用于分析山石云鉴主机安全管理系统的Syslog日志）、常规日志类关联分析和异常流量类关联分析，其中的网络威胁日志类关联分析、主机威胁日志类关联分析和常规日志类关联分析都包含多个默认关联分析规则，不可删除。除此之外，不同类型的威胁关联分析可以创建不同的自定义规则来进行相关的关联分析。

当来自于网络设备、流量探针、用户主机的数据匹配威胁引擎时，智源平台将检测到该引擎对应类型的威胁，并在"威胁" 在第115页页面展示相关威胁事件。

默认引擎

点击“引擎管理 > 威胁引擎 ”，打开威胁引擎页面，点击<默认引擎>标签页，打开默认引擎页面。



- 点击左侧栏的引擎类型，右侧窗口显示该类型的多个规则。
- 点击右上角的引擎配置切换。系统支持3种引擎模式，分别是“自定义配置”、“常规配置”和“精准配置”。用户可根据需要在下拉框中点击启用按钮选择使用的引擎。默认为“自定义配置”。自定义配置引擎下支持修改规则参数，常规配置引擎和精准配置引擎均不支持修改规则参

数。

- 自定义配置—在自定义配置下，用户可以根据实际需要修改规则参数。点击  按钮，在弹出框中选择将所有规则的参数重置为常规默认配置或精准默认配置。点击指定规则部分的  按钮，打开编辑页面，编辑所选规则的参数信息。在编辑页面点击“恢复默认”，在弹出框中选择将该规则的参数重置成常规默认配置或精准默认配置。
- 常规配置—在常规配置下，引擎的相关配置阈值较为均衡，因此可能会产生部分误报。该配置下不允许修改规则的参数信息。从自定义配置切换为常规配置时，修改的参数信息会被保存，点击  按钮，将所有规则的参数重置为常规默认配置。
- 精准配置—在精准配置下，引擎的相关配置阈值较高，因此产生的误报较少。该配置下不允许修改规则的参数信息。从自定义配置切换为精准配置时，修改的参数信息会被保存，点击  按钮，将所有规则的参数重置为精准默认配置。

  注意:

  - 威胁情报类规则由威胁情报库自动生成，不受引擎配置切换功能影响；
  - 切换/重置引擎配置时不会影响规则已产生的命中/误报次数；
  - 系统初始安装时自定义配置引擎将使用精准配置的规则参数，同时系统升级时将会保存自定义配置的规则参数。

- 启用或禁用所有规则，点击页面右上角“全选” 复选框，然后点击  或  按钮；批量启用或禁用部分规则，点击指定规则部分右上角的复选框，然后点击  或  按钮。
- 在页面右上角搜索框中输入规则名称关键字，可以对所有规则进行模糊搜索。
- 点击命中次数对应的数字跳转到威胁事件页面，系统将根据规则名称作为筛选条件筛选对应的威胁事件，显示在综合视角的威胁事件列表中；点击误报次数对应的数字跳转到威胁事件页面，系统将根据规则名称和状态作为筛选条件筛选对应的威胁事件，显示在综合视角的威胁事件列表中。

- 点击指定规则部分的按钮，打开详细信息页面，查看该规则的命中次数、误报次数、级别、检测周期等参数。在详细信息页面，点击“编辑”按钮，编辑所选规则；点击“关闭”按钮，关闭该页面。
- 点击指定规则部分的按钮，启用或禁用指定规则。

编辑默认规则

编辑指定默认规则，请按照以下步骤进行操作：

1. 点击“引擎管理 > 威胁引擎”，在威胁引擎页面，点击<默认引擎>标签页。
2. 在默认引擎页面，点击左侧栏的引擎类型（以扫描类为例），右侧窗口显示该类型的多个规则。点击指定规则（以遭受SYN端口扫描攻击为例）部分的按钮，打开编辑页面。



编辑相关配置信息。

选项	说明
规则状态	启用或禁用遭受SYN端口扫描攻击规则。
命中次数	当检测到匹配该威胁规则的数据时，命中次数自动加1。编辑该规则后，命中次数清零。
误报次数	当手动将相关威胁事件标记为误报时，误报次数自动更新。编辑该规则后，误报次数清零。
级别	指定匹配该规则的威胁的级别为严重、高危、中危或低危。

选项	说明
	默认级别为低危。
检测周期	指定系统周期性检测威胁的时间，包括60秒、120秒、300秒、600秒或自定义。默认检测周期为300秒。自定义的取值范围为1到600秒。启用该规则后： • 如果在指定检测周期内没有检测到威胁，重新计算检测周期。 • 如果在指定检测周期内检测到威胁，从检测到威胁时开始，重新计算检测周期。
次数	指定检测周期内端口被扫描的次数，包括100次、500次、1000次、2000次或自定义。默认次数为1000次。自定义的取值范围为1到2000次。
遭受扫描端口数	指定检测周期内被扫描的端口的个数，包括32、64、128、256或自定义。默认个数为32个。自定义的取值范围为1到256。
恢复默认	点击“恢复默认”按钮，恢复默认值。

3. 点击“保存”按钮完成配置。当在指定检测周期内，被扫描数超过指定次数，且被扫描的端口数超过指定个数时，系统将认为发生了威胁。例如：在300秒内，被扫描数超过1000次，被扫描端口数超过32个时，系统将认为遭受SYN端口扫描攻击。

配置保护对象

对于“违规访问类”威胁引擎规则中的“应用违规访问”规则，用户通过需要配置规则中的保护对象来指定应用访问黑/白名单，检测流量是否存在恶意访问指定的应用服务资源，从而产生威胁事件来告知用户相关的应用违规访问行为。

点击“新保护对象”按钮，在打开的<新增保护对象>页面指定对象的IP地址、启用/禁用保护对象。

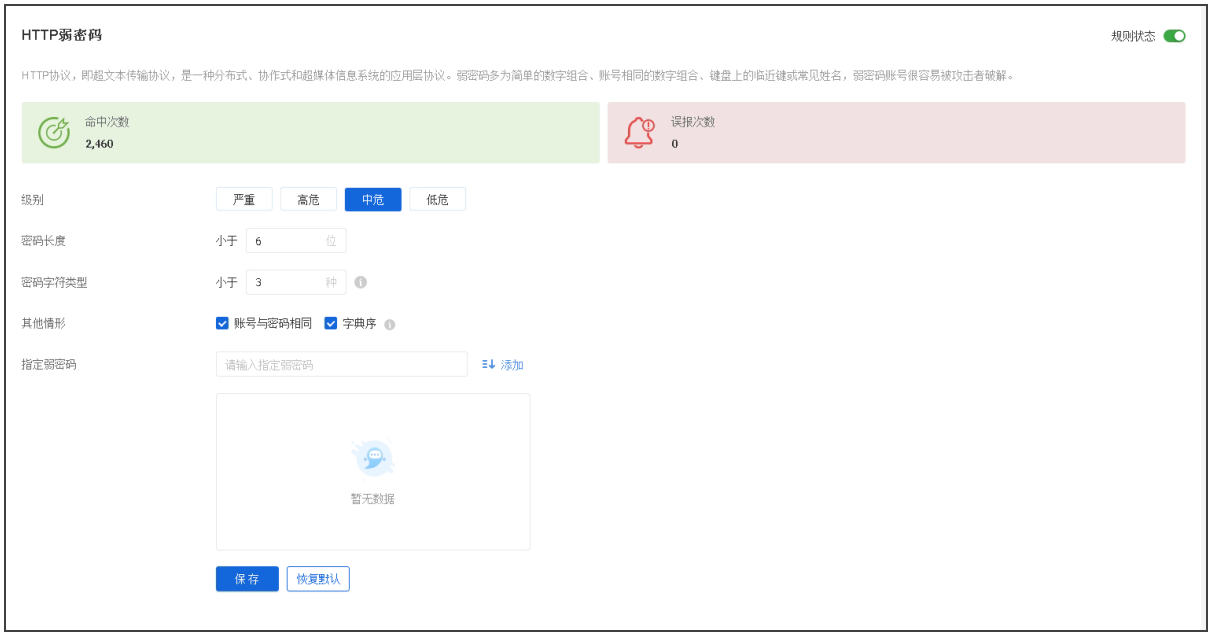
编辑弱密码检测规则

对于“弱密码检测类”威胁引擎规则，包含6类默认规则，分别为HTTP弱密码、TELNET弱密码、SMTP弱密码、POP3弱密码、IMAP弱密码、FTP弱密码，可对以上6种明文传输用户名密码的协议进行弱密码检测，及时产生对应的威胁事件，以提示用户使用弱密码导致的安全隐患。

用户可以通过修改默认规则的配置，自定义弱密码检测规则，请按照以下步骤进行操作：

1. 点击“引擎管理 > 威胁引擎”，在威胁引擎页面，点击<默认引擎>标签页。

2. 点击左侧栏的引擎类型“弱密码检测类”，右侧窗口显示该类型的多个规则。点击指定规则的 按钮，打开编辑页面。



编辑相关配置信息。

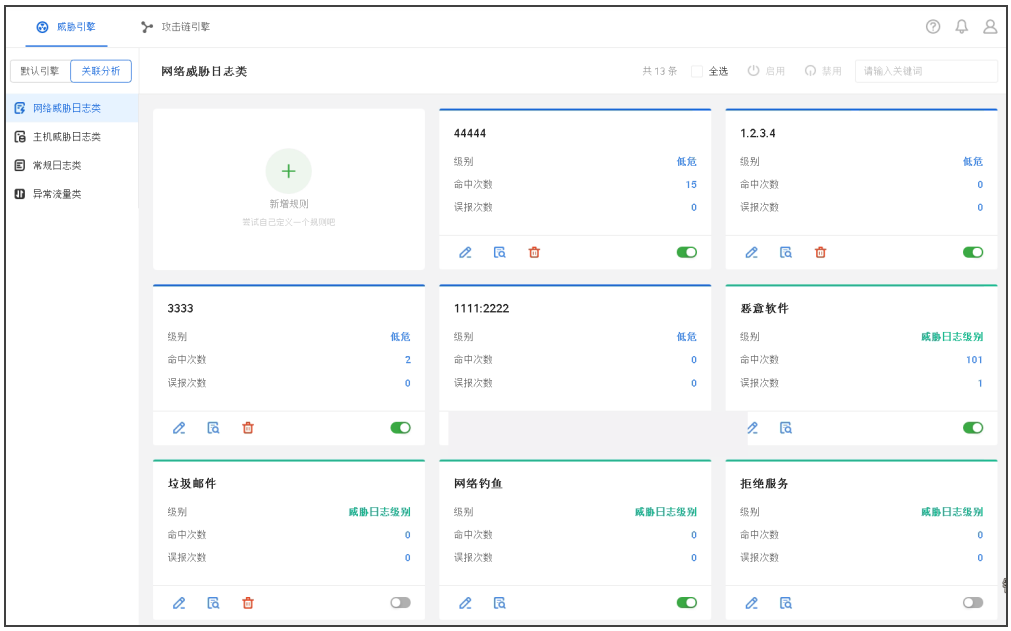
选项	说明
规则状态	启用或禁用弱密码检测规则。
命中次数	当检测到匹配该威胁规则的数据时，命中次数自动加1。编辑该规则后，命中次数清零。
误报次数	当手动将相关威胁事件标记为误报时，误报次数自动更新。编辑该规则后，误报次数清零。
级别	指定匹配该规则的威胁的级别为严重、高危、中危或低危。默认级别为中危。
密码长度	指定匹配该规则的密码长度。例如指定为“小于6位”，即当用户密码长度小于6位时，将会匹配该弱密码检测规则。
密码字符类型	指定匹配该规则的密码字符类型。字符类型共包含4种：数

选项	说明
	字、大写字母、小写字母、特殊字符。例如指定为“小于3中”，即当用户密码字符类型少于3种时，将会匹配该弱密码检测规则。
其他情形	指定匹配该规则的其他密码限制： • 账号与密码相同：当用户账号与密码相同时，将会匹配该弱密码检测规则。 • 字典序：当用户密码为顺序（升序、降序）的数字或大小写字母时，将会匹配该弱密码检测规则。
指定弱密码	指定匹配该规则的弱密码。当用户密码与指定的弱密码相同时，将会匹配该弱密码检测规则。在文本框输入特定的弱密码内容，点击“添加”按钮进行添加。

3. 点击“保存”按钮完成配置。当用户密码与规则配置中任意一个条件相匹配时，均会产生相对应的威胁事件。

关联分析

点击“引擎管理 > 威胁引擎 ”，在威胁引擎页面，点击<关联分析>标签页，打开关联分析页面。



- 点击左侧栏的关联分析类型，右侧窗口显示该类型的所有已配置规则。
- 启用或禁用所有规则，点击页面右上角“全选”复选框，然后点击  或  按钮；批量启用或禁用部分规则，点击指定规则部分右上角的复选框，然后点击  或  按钮。
- 在页面右上角搜索框中输入规则名称关键字，可以对所有关联分析规则进行模糊搜索。
- 规则面板展示规则的名称、级别、命中次数以及误报次数。
  - 点击默认规则面板中命中次数对应的数字跳转到威胁事件页面，系统将根据规则名称作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中。
  - 点击默认规则面板中误报次数对应的数字跳转到威胁事件页面，系统将根据规则名称和状态作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中。
  - 点击自定义规则面板中命中次数对应的数字，若自定义规则选择以原始日志的威胁名称作为事件名称，则跳转到威胁事件页面后，在威胁事件列表中展示全部威胁事件；若自定义规则选择以规则名称作为事件名称，则跳转到威胁事件页面后，系统将根据规则名称作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中。
  - 点击自定义规则面板中误报次数对应的数字，若自定义规则选择以原始日志的威胁名称作为事件名称，则跳转到威胁事件页面后，系统将根据状态作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中；若自定义规则选择以规则名称作为事件名称，则跳转到威胁事件页面后，系统将根据规则名称和状态作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中。
- 点击指定规则部分的  按钮，打开编辑页面，编辑所选规则的参数信息。
- 点击指定规则部分的  按钮，打开详细信息页面，查看规则、状态名称、攻击阶段等参数。在详细信息页面，点击“编辑”按钮，编辑所选规则；点击“关闭”按钮，关闭该页面。
- 点击指定自定义规则部分的  按钮，删除指定自定义规则。
- 点击指定规则部分的  按钮，启用或禁用指定规则。

新建自定义规则

新建自定义关联分析规则，请按照以下步骤进行操作：

1. 点击“引擎管理 > 威胁引擎”，在威胁引擎页面，点击<关联分析>标签页。

2. 在关联分析页面，点击左侧栏的关联分析类型，右侧窗口显示该关联分析类型的所有已配置规则。点击“新规则”按钮，打开<新增网络威胁日志规则>页面（图示以网络威胁日志类为例）。



配置相关信息。

选项	说明
状态	点击启用按钮，启用或禁用该网络威胁日志规则。
触发条件（网络威胁日志类）	

触发规则（必填项）	指定产生威胁事件的触发规则。
	• 若选择“单条触发”，智源平台每采集一条匹配该规则触发条件的网络威胁日志，则产生一个对应的威胁事件；
	• 若选择“聚合触发”，可在下方勾选需要的“聚合方式”，可多选：
	  • 按威胁名称聚合：在检测周期内，当智源平台采集的威胁名称相同的网络威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	  • 按源IP聚合：在检测周期内，当智源平台采集的源IP相同的网络威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	  • 按目的IP聚合：在检测周期内，当智源平台采集的目的IP相同的网络威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	注意：
	• 如选择多种聚合方式，将会按照所选的所有聚合方式产生威胁事件。例如：选择“按威胁名称聚合”和“按源IP聚合”，那么在检测周期内，当智源平台采集的源IP相同、威胁名称也相同的网络威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	• 如不指定任何聚合方式，则在检测周期内，当智源平台采集的网络威胁日志达到指定次数，且满足触发条件，则产生一个对应的威胁事件。

检测周期（必	当触发规则指定为“聚合触发”时，需指定系统周期性检查

选项	说明
填项）	威胁的时间，取值范围为1到10分钟。 • 启用该规则后，如果在指定检测周期内检测到威胁，从检测到威胁时开始，重新计算检测周期。 • 启用该规则后，如果在指定检测周期内没有检测到威胁，重新计算检测周期。
次数（必填项）	当触发规则指定为“聚合触发”时，需指定检测周期内产生威胁事件需要匹配的日志条目数，取值范围为1到2000。
安全设备主机IP	产生威胁事件安全设备主机IP地址。
威胁名称	指定产生威胁事件需要匹配的网络威胁日志中的威胁名称。
威胁日志大类	指定产生威胁事件需要匹配的网络威胁日志大类，可多选。
威胁日志级别	指定产生威胁事件需要匹配的网络威胁日志级别，可多选。
动作	指定产生威胁事件需要匹配的网络威胁日志的动作，可多选。
源IP地址/掩码	指定产生威胁事件需要匹配的网络威胁日志的源地址。可指定为IPv6地址。
目的IP地址/掩码	指定产生威胁事件需要匹配的网络威胁日志的目的地址。可指定为IPv6地址。
当采集的数据匹配触发条件时，系统判断其命中该规则。例如，在触发条件中，触发规则选择“聚合触发”，聚合方式指定为“按源IP聚合”，检测周期为5分钟，次数为10次。指定安全设备主机IP为10.180.188.35，威胁日志大类选择“网络钓鱼类”，威胁日志级别选择所有级别，那么在5分钟内，系统检测到地址为10.180.188.35的安全设备生成了源IP相同的网络钓鱼类日志（所有级别）的条目数超过10，将认为发生了威胁。	
触发条件（主机威胁日志类）	
触发规则（必填项）	指定产生威胁事件的触发规则。 • 若选择“单条触发”，智源平台每采集一条匹配该规则

选项	说明

	触发条件的主机威胁日志，则产生一个对应的威胁事件；
	• 若选择“聚合触发”，可在下方勾选需要的“聚合方式”，可多选：
	  • 按威胁名称聚合：在检测周期内，当智源平台采集的威胁名称相同的主机威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	  • 按源IP聚合：在检测周期内，当智源平台采集的源IP相同的主机威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	  • 按目的IP聚合：在检测周期内，当智源平台采集的目的IP相同的主机威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	注意：
	• 如选择多种聚合方式，将会按照所选的所有聚合方式产生威胁事件。例如：选择“按威胁名称聚合”和“按源IP聚合”，那么在检测周期内，当智源平台采集的源IP相同、威胁名称也相同的主机威胁日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	• 如不指定任何聚合方式，则在检测周期内，当智源平台采集的主机威胁日志达到指定次数，且满足触发条件，则产生一个对应的威胁事件。

检测周期（必填项）	当触发规则指定为“聚合触发”时，需指定系统周期性检查威胁的时间，取值范围为1到10分钟。 • 启用该规则后，如果在指定检测周期内检测到威胁，从检测到威胁时开始，重新计算检测周期。 • 启用该规则后，如果在指定检测周期内没有检测到威

选项	说明
	胁，重新计算检测周期。
次数（必填项）	当触发规则指定为“聚合触发”时，需指定检测周期内产生威胁事件需要匹配的日志条目数，取值范围为1到2000。
安全设备主机IP	产生威胁事件安全设备主机IP地址。
威胁名称	指定产生威胁事件需要匹配的主机威胁日志中的威胁名称。
威胁日志级别	指定产生威胁事件需要匹配的主机威胁日志级别，可多选。
动作	指定产生威胁事件需要匹配的主机威胁日志的动作，包括阻止并隔离、阻止、仅记录、不处理，可多选。
源IP地址/掩码	指定产生威胁事件需要匹配的主机威胁日志的源地址。可指定为IPv6地址。
目的IP地址/掩码	指定产生威胁事件需要匹配的主机威胁日志的目的地址。可指定为IPv6地址。
触发条件（常规日志类）	
日志类型（必填项）	指定产生威胁事件需要匹配的日志类型，常规日志包括6种日志类型：URL日志、上网行为审计日志、防篡改日志、文件过滤日志、网页安全日志、内容过滤日志。

触发规则（必填项）	指定产生威胁事件的触发规则。
	• 若选择“单条触发”，智源平台每采集一条匹配该规则触发条件的常规日志，则产生一个对应的威胁事件；
	• 若选择“聚合触发”，可在下方勾选需要的“聚合方式”，可多选：
	  • 按日志名称聚合：在检测周期内，当智源平台采集的名称相同的常规日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。
	  • 按源IP聚合：在检测周期内，当智源平台采集的源IP相同的常规日志条目数达到触发条件指定的次

选项	说明
	数，则产生一个对应的威胁事件。 • 按目的IP聚合：在检测周期内，当智源平台采集的目的IP相同的常规日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。 **注意**: • 如选择多种聚合方式，将会按照所选的所有聚合方式产生威胁事件。例如：选择“按威胁名称聚合”和“按源IP聚合”，那么在检测周期内，当智源平台采集的源IP相同、威胁名称也相同的常规日志条目数达到触发条件指定的次数，则产生一个对应的威胁事件。 • 如不指定任何聚合方式，则在检测周期内，当智源平台采集的常规日志达到指定次数，且满足触发条件，则产生一个对应的威胁事件。
检测周期（必填项）	当触发规则指定为“聚合触发”时，需指定系统周期性检查威胁的时间，取值范围为1到10分钟。 • 启用该规则后，如果在指定检测周期内检测到威胁，从检测到威胁时开始，重新计算检测周期。 • 启用该规则后，如果在指定检测周期内没有检测到威胁，重新计算检测周期。
次数（必填项）	当触发规则指定为“聚合触发”时，需指定检测周期内产生威胁事件需要匹配的所选日志类型条目数，取值范围为1到2000。
安全设备主机IP	产生威胁事件安全设备主机IP地址。
日志名称	指定产生威胁事件需要匹配的日志名称。
日志级别	指定产生威胁事件需要匹配的日志级别，可多选。
动作	指定产生威胁事件需要匹配的所选类型日志的动作，可多

选项	说明
	选。
源IP地址/掩码	指定产生威胁事件需要匹配的所选日志类型的源地址。可指定为IPv6地址。
目的IP地址/掩码	指定产生威胁事件需要匹配的所选日志类型的目的地址。可指定为IPv6地址。
触发条件（异常流量类）	

检测类型	指定产生威胁事件需要匹配的异常流量检测类型。不同检测类型所对应的触发条件不同。
	• **超出阈值检测**：在“检测周期”内，如果系统检测到IP地址为“服务器”IP的安全设备流量超过“流量阈值”，产生异常流量威胁事件。
	  • 服务器：指定被检测的服务器。点击下拉菜单选择已配置的服务器名称。
	  • 检测周期：指定检测时间周期。范围是1-10分钟。
	  • 流量阈值：指定产生异常流量威胁事件需要匹配的流量阈值大小。范围是1-102400MB。
	• **流量突峰检测**：在“检测粒度”时间范围内，如果系统检测到在“IP网段”内的安全设备的流量突然上升，结合指定的“告警敏感值”，产生异常流量威胁事件。
	  • IP网段：指定IP地址类型（IPv4或IPv6）以及输入需要进行流量突变检测的网段的起始IP和终止IP，并点击“添加网段”按钮，添加IP地址段。用户可添加多个IP地址段。
	  • 检测粒度：指定检测时间粒度。范围是5-10分钟。
	  • 告警敏感值：指定对异常流量的检测敏感度。范围是1-100。敏感值越大，产生威胁事件的几率越

选项	说明

	大。
	• **流量突降检测**：在“检测粒度”时间范围内，如果系统检测到在“IP网段”内的安全设备的流量突然下降，结合指定的“告警敏感值”，产生异常流量威胁事件。
	  • IP网段：指定IP地址类型（IPv4或IPv6）以及输入需要进行流量突变检测的网段的起始IP和终止IP，并点击“添加网段”按钮，添加IP地址段。用户可添加多个IP地址段。
	  • 检测粒度：指定检测时间粒度。范围是5-10分钟。
	  • 告警敏感值：指定对异常流量的检测敏感度。范围是1-100。敏感值越大，产生威胁事件的几率越大。
	注意：
	• 同一个异常流量规则中支持同时开启流量突峰检测和流量突降检测。
	• 当告警敏感值设置越大的时候，检测的精确度很高，因此，产生误报的可能性也就越大，请根据实际要求设置。

规则描述	
规则名称（必填项）	指定威胁日志规则的名称。
威胁展示名称	指定威胁事件的展示名称。 • 若选择“规则名称”，则以该威胁日志规则的名称作为匹配规则的威胁事件名称； • 若选择“源威胁名称”，则以原始日志的威胁名称作为匹配规则的威胁事件名称。

选项	说明
攻击阶段	指定匹配该规则的威胁所处的攻击阶段。 当未指定任何攻击阶段时，在产生威胁事件的同时，系统会根据该事件的攻击方向和威胁标签自动判断攻击阶段并加入威胁事件详细信息中。
展示级别	指定匹配该规则的威胁事件的展示级别。 • 若选择“指定级别”，匹配该规则的威胁事件级别将使用指定的“威胁级别”展示（严重、高、中、或低）。 • 若选择“威胁日志级别”，匹配该规则的威胁事件级别将使用威胁日志的级别展示。
描述	输入规则的描述信息。
建议	输入规则的建议信息。

3. 点击“保存”按钮完成配置。



注意: 系统最多支持存储200条网络威胁日志类关联分析规则、200条主机威胁日志类关联分析规则、200条常规日志类关联分析规则和5条异常流量类关联分析规则。

攻击链引擎

智源平台提供默认攻击链引擎（多个威胁事件类型组成的引擎）和攻击链关联分析。

- 默认攻击链引擎：由引擎库提供，包括异常登录类和勒索类。每个类型的默认攻击链引擎都包含一个或多个默认攻击链规则，用户可直接使用或编辑后使用默认攻击链规则，但不可以删除默认攻击链引擎和其包含的规则。
- 攻击链关联分析：用来分析智源平台采集到的日志信息。攻击链关联分析包括威胁事件类关联分析，可创建自定义规则来进行相关的关联分析。

当来自于网络设备、流量探针和用户主机的数据匹配攻击链引擎时，智源平台将检测到该引擎对应类型的威胁，并在"威胁" 在第115页页面展示相关威胁事件。

默认引擎

点击“引擎管理 > 攻击链引擎 ”，在攻击链引擎页面，点击<默认引擎>标签页，打开默认引擎页面。



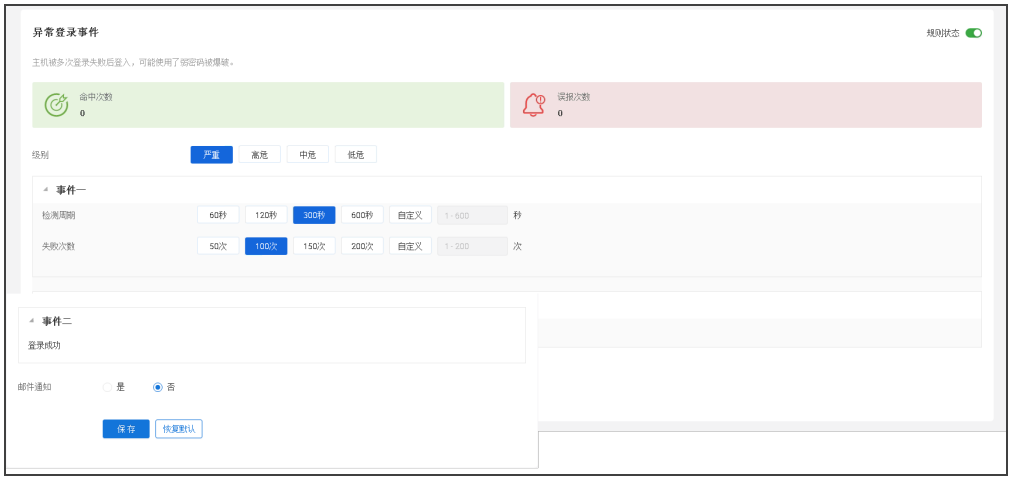
- 点击左侧栏的引擎类型，右侧窗口显示该类型的规则。
- 启用或禁用所有规则，点击页面右上角“全选” 复选框，然后点击 启用 或 禁用 按钮；批量启用或禁用部分规则，点击指定规则部分右上角的复选框，然后点击 启用 或 禁用 按钮。
- 在页面右上角搜索框中输入规则名称关键字，可以对所有规则进行模糊搜索。
- 点击命中次数对应的数字跳转到威胁事件页面，系统将根据规则名称作为筛选条件筛选对应的威胁事件，显示在综合视角的威胁事件列表中；点击误报次数对应的数字跳转到威胁事件页面，系统将根据规则名称和状态作为筛选条件筛选对应的威胁事件，显示在综合视角的威胁事件列表中。

- 点击指定规则部分的按钮，打开编辑页面，编辑所选规则的参数信息。
- 点击指定规则部分的按钮，打开详细信息页面，查看命中次数、误报次数、级别等参数。在详细信息页面，点击“编辑”按钮，编辑所选规则；点击“关闭”按钮，关闭该页面。
- 点击指定规则部分的按钮，启用或禁用指定规则。

编辑默认规则

编辑指定规则，请按照以下步骤进行操作：

1. 点击“引擎管理 > 攻击链引擎”，在攻击链引擎页面，点击<默认引擎>标签页。
2. 在默认引擎页面，点击左侧栏的引擎类型（以异常登录类为例），右侧窗口显示该类型的规则。点击指定规则（以异常登录事件为例）部分的按钮，打开编辑页面。



编辑相关配置信息。

选项	说明
规则状态	点击右上角启用按钮，启用或禁用异常登录事件规则。
命中次数	当检测到匹配该威胁规则的数据时，命中次数自动加1。编辑该规则后，命中次数清零。
误报次数	当手动将相关威胁事件标记为误报时，误报次数自动更新。编辑该规则后，误报次数清零。
级别	指定命中该规则的威胁的级别为严重、高、中或低。

事件一	指定产生威胁事件的第一个触发条件。
	• 检测周期：指定系统周期性检测威胁的时间，包括60秒、120秒、300秒、600秒或自定义。自定义的取值范围为1到600秒。
	  • 启用该规则后，如果在指定检测周期内没有检测到威胁，重新计算检测周期。
	  • 启用该规则后，如果在指定检测周期内检测到威胁，从检测到威胁时开始，重新计算检测周期。
	• 失败次数：指定检测周期内登录主机失败的次数，包括50次、100次、150次、200次或自定义。自定义的取值范围为1到200次。

事件二	显示产生威胁事件的第二个触发条件为“登录成功”。
恢复默认	点击“恢复默认”按钮，恢复默认值。
当采集的数据同时匹配事件一和事件二时，系统判断其命中该规则。例如：在300秒内，登录主机连续失败的次数超过150次，之后登录成功，系统将认为发生了威胁。	

3. 点击“保存”按钮完成配置。

关联分析

点击“引擎管理 > 攻击链引擎 ”，在攻击链引擎页面，点击<关联分析>标签页，打开关联分析页面。



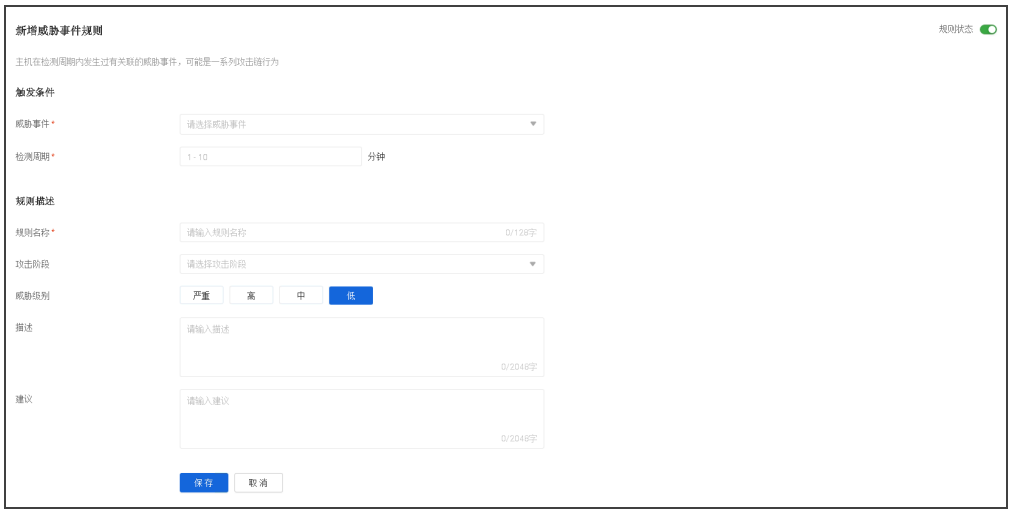
- 点击左侧栏的关联分析类型，右侧窗口显示该类型的所有已配置规则。
- 在页面右上角搜索框中输入规则名称关键字，可以对所有规则进行模糊搜索。
- 规则面板展示规则的名称、级别、命中次数以及误报次数。
    - 点击自定义规则面板中命中次数对应的数字，若自定义规则选择以原始日志的威胁名称作为事件名称，则跳转到威胁事件页面后，在威胁事件列表中展示全部威胁事件；若自定义规则选择以规则名称作为事件名称，则跳转到威胁事件页面后，系统将根据规则名称作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中。
    - 点击自定义规则面板中误报次数对应的数字，若自定义规则选择以原始日志的威胁名称作为事件名称，则跳转到威胁事件页面后，系统将根据状态作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中；若自定义规则选择以规则名称作为事件名称，则跳转到威胁事件页面后，系统将根据规则名称和状态作为筛选条件筛选对应的威胁事件，显示在威胁事件列表中。
- 点击指定规则部分的按钮，打开编辑页面，编辑所选规则的参数信息。
- 点击指定规则部分的按钮，打开详细信息页面，查看命中次数、误报次数、级别等参数。在详细信息页面，点击“编辑”按钮，编辑所选规则；点击“关闭”按钮，关闭该页面。
- 点击指定规则部分的按钮，删除指定规则。
- 点击指定规则部分的按钮，启用或禁用指定规则。

新建自定义规则

新建自定义关联分析规则，请按照以下步骤进行操作：

1. 点击“引擎管理 > 攻击链引擎”，在攻击链引擎页面，点击<关联分析>标签页。

2. 在关联分析页面，点击左侧栏的关联分析类型，右侧窗口显示所有已配置规则。点击“新规则”按钮，打开<新威胁事件规则>页面。



配置相关信息。

选项	说明
规则状态	点击右上角启用按钮，启用或禁用该攻击链规则。
触发条件	
威胁事件	指定产生自定义威胁事件需要同时匹配的威胁事件类型，可多选。
检测周期	指定系统周期性检查威胁的时间，取值范围为1到10分钟。 • 如果在指定检测周期内没有检测到威胁，重新计算检测周期。 • 如果在指定检测周期内检测到威胁，从检测到威胁时开始，重新计算检测周期。
规则描述	
规则名称（必填项）	指定攻击链规则的名称。
攻击阶段	指定命中该攻击链规则的威胁所处的攻击阶段。
威胁级别	指定命中该攻击链规则的威胁的级别为严重、高、中或低。默认级别为低。
描述	输入攻击链规则的描述信息。
建议	输入攻击链规则的建议信息。
当采集的数据匹配触发条件时，系统判断其命中该规则。例如，在10分钟内检测到可疑的PE（可执行文件）下载和TELNET暴力破解威胁事件，系统将认为受到了威胁。	

3. 点击“保存”按钮完成配置。



注意: 系统最多支持存储3条威胁事件类关联分析规则。

第11章 日志管理

日志管理页面包含如下内容：

- "日志源管理" 在第409页：介绍如何在智源平台管理日志数据源以及如何新建日志源。
- "日志解析" 在第411页：介绍如何配置日志解析规则、日志解析配置以及预定义日志解析配置的升级。
- "日志存储管理" 在第434页：介绍如何查看智源平台的存储空间、备份日志信息以及查看备份日志信息。
- "日志设备" 在第441页：介绍如何查看最近一天内向智源平台发送了Sysmon日志信息的用户主机设备信息。
- "日志服务器" 在第442页：介绍如何新建、编辑或删除日志服务器。

日志源管理

智源平台可以采集到大量来自于山石网科安全设备、流量探针、威胁探针和用户主机的日志信息，随之可能会遭受到部分威胁攻击。为了避免该问题，用户可以配置可信的日志源对数据源进行控制，使得用户能够直接在智源平台管理数据源，从而进一步保证系统安全。

点击“日志管理”，选择<日志源管理>标签页，打开日志源管理页面。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的日志源。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 列表中“Syslog”、“NetFlow”栏显示智源平台接收日志源的Syslog或NetFlow类型日志的开启状态。 表示启用， 表示禁用。
- 点击列表中日志源条目后的 按钮，打开“编辑日志源”页面，编辑所选日志源。
- 点击列表中日志源条目后的 按钮，删除所选日志源。如需批量删除日志源，勾选多个日志源条目，点击“删除”按钮。
- 点击“新日志源”按钮，创建日志源，详细步骤请参阅新建日志源。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新日志源列表。

新建日志源

新增日志源，请按照以下步骤进行操作：

1. 选择“日志管理”。
2. 选择<日志源管理>标签页。

3. 点击“新日志源”按钮，打开“新日志源”页面。



在“新日志源”页面，填写日志源配置信息。

选项	说明
名称（必填项）	指定日志源的名称。
类型	指定日志源地址类型，选择“IP地址”或“IP范围”单选按钮。 • IP地址：在“IP地址”文本框中分别输入日志源的IP地址。 • IP范围：在“IP范围”文本框中分别输入日志源的起始IP地址和终止IP地址。
接收日志	启用或禁用智源平台接收日志源的Syslog类型日志、NetFlow类型日志。
备注	指定日志源的备注信息。

4. 点击“确定”按钮完成配置。

日志解析

智源平台可以采集到来自于山石网科安全设备或者第三方网络设备的Syslog类型日志信息，由于第三方网络设备的Syslog日志信息的格式并非与智源平台日志格式相一致，为了能够在智源平台展示该日志信息，因此，系统提供了日志解析功能。用户可以根据当前网络设备日志格式创建自定义日志解析规则，系统将会实时解析收到的第三方网络设备Syslog日志信息，解析后展示在智源平台中（"第3章 威胁分析" 在第114页>"日志" 在第146页）。

同时日志解析功能还支持威胁日志的标准化，将第三方网络设备的日志转换为山石网科设备的标准威胁日志格式，以便在智源平台中展示相应的威胁事件（"第3章 威胁分析" 在第114页>"威胁" 在第115页>"事件列表" 在第136页）。

日志解析功能的配置流程如下：

1. 升级智源日志解析配置特征库，更新预定义日志解析配置。
2. 新建自定义日志解析配置。
3. 新建日志解析模板，并在日志解析模板中配置日志解析流程或者配置威胁日志标准化。
4. 新建日志解析规则并引用日志解析配置。

相关链接：

- "日志解析配置" 在第412页
- "配置日志解析规则" 在第430页

日志解析配置

日志解析配置包括预定义日志解析配置和自定义日志解析配置。

- 预定义日志解析配置：针对常用的第三方网络设备，智源平台系统包含多种预定义的日志解析配置以及对应的日志解析模板。用户可以通过升级智源日志解析配置特征库，获取最新的预定义日志解析配置，并且可以在日志解析规则中直接引用该预定义日志解析配置。
- 自定义日志解析配置：用户可以根据当前所使用的第三方网络设备Syslog日志信息的格式，创建自定义日志解析配置、对应的日志解析模板，通过使用指定的解析流程（Grok解析、Key-Value解析、JSON解析）对Syslog日志信息的解析。



注意:

- 预定义日志解析配置仅支持查看，不可修改或删除。
- 关于智源日志解析配置特征库升级方式，请参阅日志解析配置特征库升级。

日志解析配置特征库升级

智源日志解析配置特征库支持在线升级和离线升级两种方式。用户可根据自身的网络环境进行选择。

在线升级

当设备与互联网相连，能访问到智源日志解析配置特征库升级服务器时，建议用户采用在线升级的方式进行升级。

智源日志解析配置特征库的在线升级，请按照以下步骤进行操作：

1. 选择“日志管理>日志解析”。
2. 选择<日志解析配置>标签页。
3. 点击“配置升级管理”，打开<日志解析配置升级>页面。

4. 在线升级支持手动升级和定时升级两种方式。
    - 手动升级：点击“立即升级”按钮，立即升级智源日志解析配置特征库。
    - 定时升级：点击启用按钮，然后配置升级计划。可以设置“每日”或“每周”的一个固定的时间点进行升级。
5. 升级服务器设置：设备提供两个默认智源日志解析配置特征库更新服务器，输入update1.hillstonenet.com或update2.hillstonenet.com。

离线升级

当设备无法连接到互联网时，用户可以提前下载智源日志解析配置特征库文件，然后复制在本地计算机再进行离线升级。下载时，请访问网站：https://update1.hillstonenet.com和https://update2.hillstonenet.com。

智源日志解析配置特征库的离线升级，请按照以下步骤进行操作：

1. 点击“选择文件”按钮，在本地计算机选择离线升级的智源日志解析配置特征库文件（支持.sig格式）。
2. 选择文件后，点击“立即升级”按钮，系统开始上传智源日志解析配置特征库文件并开始升级。

新建自定义日志解析配置

新建自定义日志解析配置，请按照以下步骤进行操作：

1. 选择“日志管理>日志解析”。
2. 选择<日志解析配置>标签页。

3. 点击“新配置”按钮，打开<新日志解析配置>页面。



配置自定义日志解析配置相关信息。

选项	说明
名称（必填项）	指定自定义日志解析配置的名称。
类型（必填项）	点击下拉菜单选择发送Syslog日志的第三方网络设备的类型，例如：数据库、防火墙、入侵检测系统等。
型号（必填项）	指定发送Syslog日志的第三方网络设备的型号，例如：SG-6000。
描述	输入自定义日志解析配置的描述信息。

4. 点击“确定”按钮，配置完成的自定义日志解析配置将显示在列表中。

新建日志解析模板

自定义日志解析配置创建完成后，还需要配置对应的日志解析模板，在日志解析模板中指定原始日志样例、类型、配置日志解析流程、配置日志标准化。

新建日志解析模板，请按照以下步骤进行操作：

1. 选择“日志管理>日志解析”。
2. 选择<日志解析配置>标签页。
3. 在列表中选择已创建好的日志解析配置条目，点击 › 按钮，展开对应的<日志解析模板>列表页面。
4. <日志解析模板>列表页面，点击“新模板”按钮，打开<新日志解析模板>页面。
5. 在第一步“基础配置”中，配置日志解析模板基础信息。



配置日志解析模板基础信息。

选项	说明
名称（必填项）	指定日志解析模板的名称。
日志类型（必填项）	指定解析成功的日志信息在智源平台中展示的日志类型，即在“"第3章 威胁分析" 在第114页>"日志" 在第146页>Syslog”页面中对应的日志分类。
原始日志样例（必填项）	输入用户需要解析的原始日志样例。

6. 在“解析流程”部分，配置日志解析流程。

   注意：在进入到“下一步”之前，请点击解析流程中的“解析”按钮，并确保已完成解析流程验证，否则将会无法进入到下一步中。

7. 点击“下一步”，打开第二步“标准化”配置页面，根据需求开启标准化功能并进行标准化配置。
8. 完成上述配置后，可点击“解析”按钮，打开<解析结果>页面查看根据所配置的所有解析流程对原始日志的最终解析结果。
9. 如需返回上一步查看或修改解析流程配置，点击“上一步”按钮。
10. 点击“确定”按钮保存所有日志解析模板的配置信息。



注意:

- 每个自定义日志解析配置中最多允许创建50个模板。
- 同一个日志解析配置中，不同的日志解析模板不能解析同一种日志格式的日志信息，否则将会出现解析冲突的问题。

配置日志解析流程

系统支持以下三种解析方式：

- Grok解析：是一种采用组合多个预定义的正则表达式，用来匹配分割文本并映射到关键字的工具。通常用来对日志数据进行处理。
- Key-Value解析：是一种对key-value格式日志的解析工具。
- JSON解析：JSON是一种轻量级的数据交换格式。JSON解析，是一种可以把包含JSON格式的日志进行格式化解析的工具。



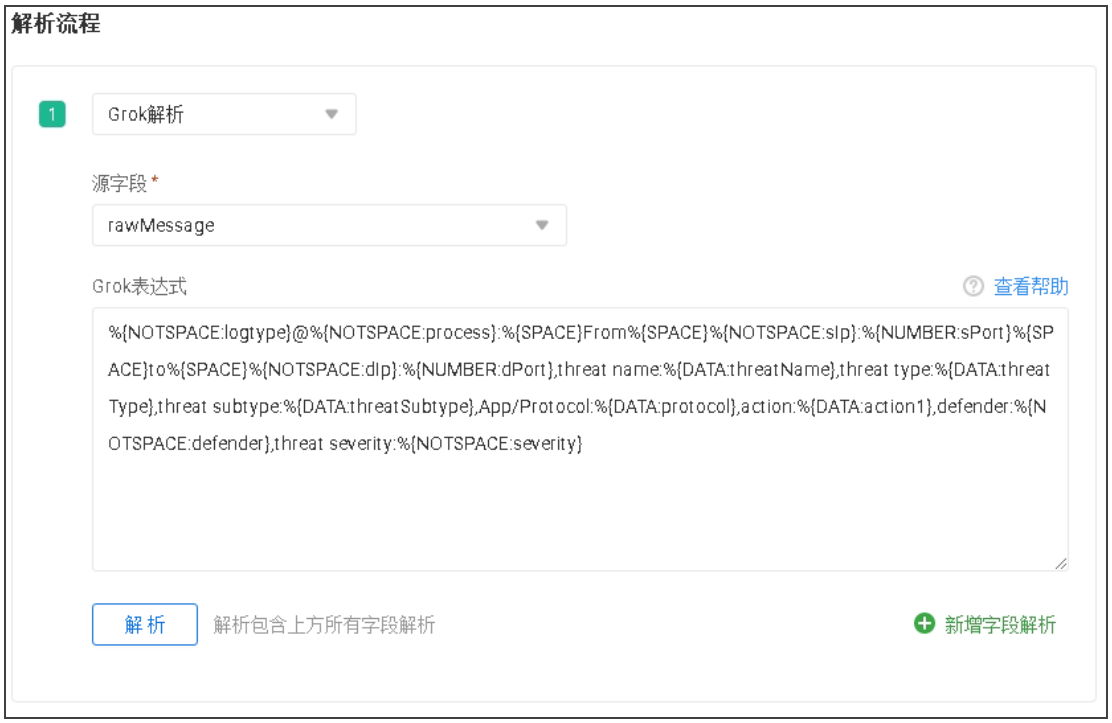
注意:

- 根据用户实际需求，同一个解析模板中可以添加多个字段解析流程。系统允许最多添加10个字段解析流程。
- 如果当前的字段解析流程未能成功解析，则不能继续添加新的字段解析流程，也不能进入到下一步配置中。

配置Grok解析流程

配置Grok解析流程，请按照以下步骤进行操作：

1. 在<新日志解析模板>页面的“解析流程”部分，点击下拉菜单选择“Grok解析”。



配置Grok解析解析相关信息。

选项	说明
源字段（必填项）	点击“源字段”下拉菜单，选择解析的源字段。 • 如果该Grok解析为解析流程的第一步，那么该“源字段”仅可选择“rawMessage”（原始日志）； • 如果该Grok解析为解析流程的第二步或之后步骤，那么该“源字段”可选择上一步解析结果中的字段。
Grok表达式	在文本框中，输入用于解析源字段内容的符合Grok语法的Grok表达式

2. 如需查看关于Grok的帮助，点击“查看帮助”按钮，在<Grok帮助栏>查看Grok的简介、常见模式、常见语法使用方法以及Grok解析举例。



3. 点击“解析”按钮，验证上述解析配置是否准确。如配置准确，将会打开<解析结果>页面，展示Grok解析的结果。



4. 点击“新增字段解析”，添加新的字段解析流程。

5. 如需删除已配置的字段解析流程，点击右上角的 按钮。

Grok解析举例如下：

假设选择的源字段内容为：

Threat@UTAD: From 111.1.1.18:1110 to 112.1.1.5:0,threat name:Firewall Policy Violation,threat type:Attack,threat subtype:Passwrod Attack,App/Protocol:-/-,action:block,defender:ABD,threat severity:High

- Grok表达式指定为：
  %{NOTSPACE:logtype}@%{NOTSPACE:process}:%{SPACE}From%{SPACE}%{NOTSPACE:sIp}:%{NUMBER:sPort}%{SPACE}to%{SPACE}%{NOTSPACE:dIp}:%{NUMBER:dPort},threat name:%{DATA:threatName},threat type:%{DATA:threatType},threat subtype:%{DATA:threatSubtype},App/Protocol:%{DATA:protocol},action:%{DATA:action1},defender:%{NOTSPACE:defender},threat severity:%{NOTSPACE:severity}

则使用Grok解析之后的解析结果为：

severity: High

process: UTAD

dPort: 0

dIp: 112.1.1.5

type: THREAT

message: Threat@UTAD: From 111.1.1.18:1110 to 112.1.1.5:0,threat name:Firewall Policy Violation,threat type:Attack,threat subtype:Passwrod Attack,App/Protocol:-/-,action:block,defender:ABD,threat severity:High

sPort: 1110

logtype: Threat

protocol: -/-

associatedLogParseTemplateName: grok示例2

threatType: Attack

threatName: Firewall Policy Violation

threatSubtype: Passwrod Attack

sIp: 111.1.1.18

action1: block

defender: ABD

配置Key-Value解析流程

配置Key-Value解析流程，请按照以下步骤进行操作：

1. 在<新日志解析模板>页面的“解析流程”部分，点击下拉菜单选择“Key-Value解析”。

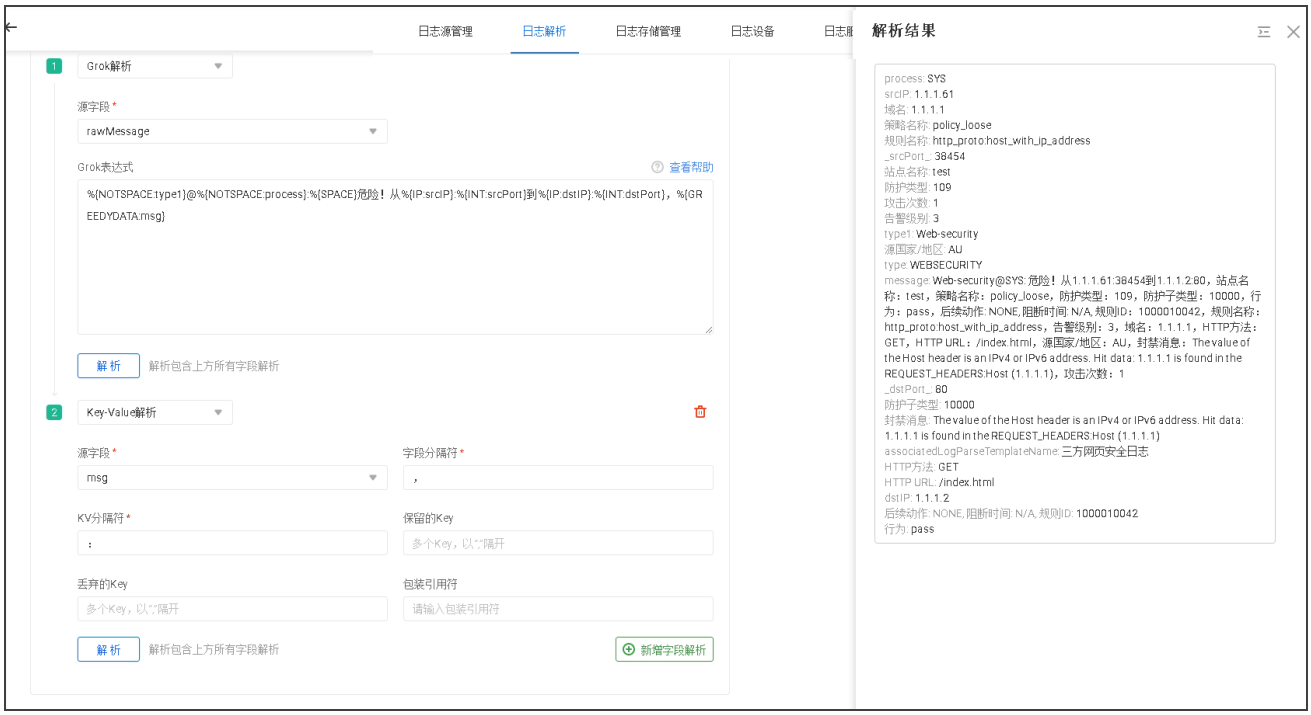


配置Key-Value解析相关信息。

选项	说明
源字段（必填项）	点击“源字段”下拉菜单，选择解析的源字段。 • 如果该Key-Value解析为解析流程的第一步，那么该“源字段”仅可选择“rawMessage”（原始日志）； • 如果该Key-Value解析为解析流程的第二步或之后步骤，那么该“源字段”可选择上一步解析结果中的字段。
字段分隔符（必填项）	指定源字段内容中各字段的分隔符。
KV分隔符（必填项）	指定Key和Value之间的分隔符。
保留的Key	指定解析结果中需要保留展示的Key。
丢弃的Key	指定解析结果中不需要保留展示的Key。 **注意**：“保留的Key”和“丢弃的Key”不允许同时配置，仅可配置一个选项。
包装引用符	指定包裹字段值引用的符号。

选项	说明
	注意：包装引用符仅对Value生效。

2. 点击“解析”按钮，验证上述解析配置是否准确。如配置准确，将会打开<解析结果>页面，展示Key-Value解析的结果。



3. 点击“新增字段解析”，添加新的字段解析流程。

4. 如需删除已配置的字段解析流程，点击右上角的 按钮。

Key-Value解析举例如下：

假设选择的源字段内容为：

"mod"="cli,administrator", from=192.168.220.2, mesg="this is a test, result=success"

- 字段分隔符指定为 ,
- KV分隔符指定为 =
- 包装引用符指定为 ” （即mesg字段值的包裹符号为双引号）

则使用Key-Value解析之后的解析结果为：

"mod": "cli,administrator"

associatedLogParseTemplateName: kv包装引用符

from: 192.168.220.2

type: WAFWEBEVENT

message: "mod"="cli,administrator", from=192.168.220.2, mesg="this is a test, result=success"

mesg: "this is a test, result=success"

配置JSON解析流程

配置JSON解析流程，请按照以下步骤进行操作：

1. 在<新日志解析模板>页面的“解析流程”部分，点击下拉菜单选择“JSON解析”。

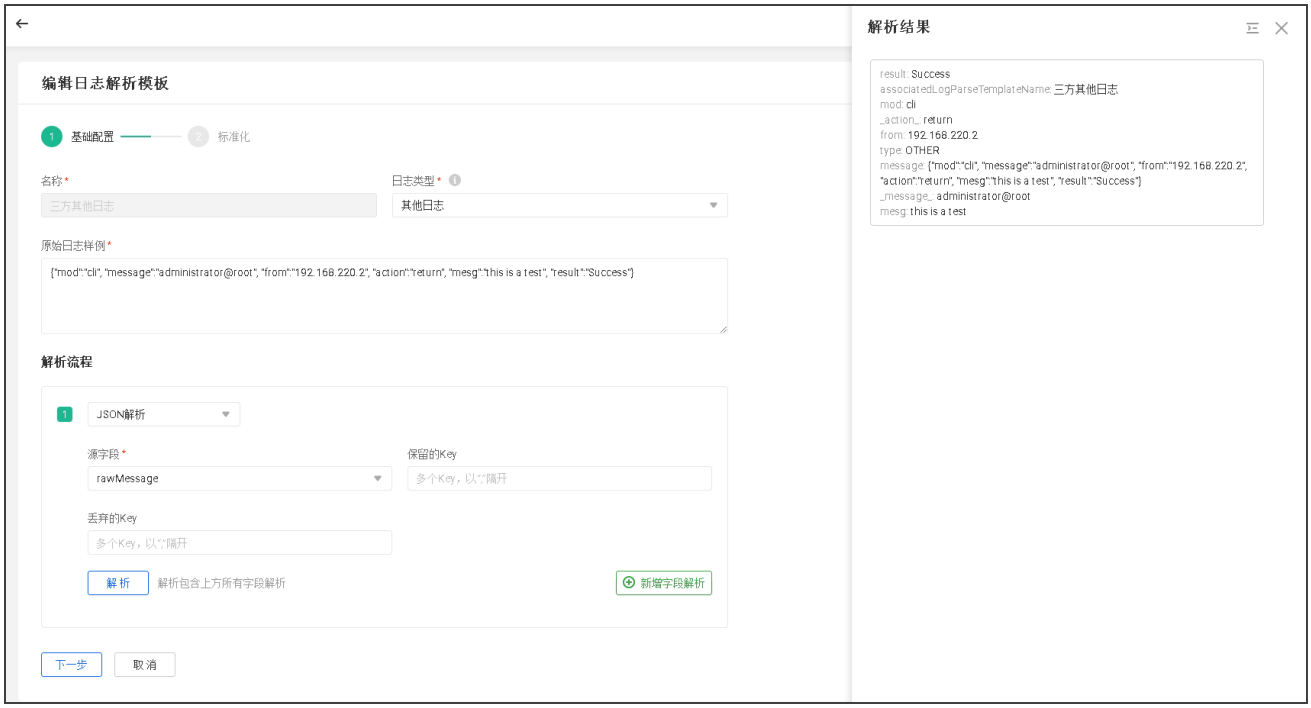


配置JSON解析相关信息。

选项	说明
源字段（必填项）	点击“源字段”下拉菜单，选择解析的源字段。 • 如果该JSON解析为解析流程的第一步，那么该“源字段”仅可选择“rawMessage”（原始日志）； • 如果该JSON解析为解析流程的第二步或之后步骤，那么该“源字段”可选择上一步解析结果中的字段。
保留的Key	指定解析结果中需要保留展示的Key。
丢弃的Key	指定解析结果中不需要保留展示的Key。

选项	说明
	注意：“保留的Key”和“丢弃的Key”不允许同时配置，仅可配置一个选项。

2. 点击“解析”按钮，验证上述解析配置是否准确。如配置准确，将会打开<解析结果>页面，展示JSON解析的结果。



3. 点击“新增字段解析”，添加新的字段解析流程。

4. 如需删除已配置的字段解析流程，点击右上角的 按钮。

JSON解析举例如下：

假设选择的源字段内容为：

"mod":"cli", "usr":"administrator@root", "from":"192.168.220.2", "action":"return", "mesg":"this is a test", "result":"Success"

- 保留的Key指定为mod, usr (用英文逗号隔开)

则使用JSON解析之后的解析结果为：

associatedLogParseTemplateName: json

mod: cli

usr: administrator@root

type: EI

message: {"mod":"cli", "usr":"administrator@root", "from":"192.168.220.2", "action":"return", "mesg":"this is a test", "result":"Success"}

调整解析流程顺序

同一个解析模板中可以添加多个字段解析流程，日志解析的顺序将会按照解析流程的顺序依次进行解析，当解析流程的个数在3个以上时，用户可以根据需求调整解析流程的顺序。

在<新日志解析模板>页面的“解析流程”部分，可以进行以下操作调整解析流程顺序：

- 向上移动：点击右上角按钮，向上移动所选的解析流程，与上一个解析流程交换顺序。
- 向下移动：点击右上角按钮，向下移动所选的解析流程，与下一个解析流程交换顺序。

注意:

- 调整解析流程顺序后，源字段的配置将会置空，用户需要重新选择源字段内容。
- 调整解析流程顺序可能导致解析失败，请谨慎操作。
- 由于第一个解析流程的源字段为“rawMessage”（原始日志），因此第一个解析流程不能执行向下移动的操作，第二个解析流程不能执行向上移动的操作。
- 最后一个解析流程仅可执行向上移动的操作。

配置日志标准化

日志的标准化，包括标准化映射和自定义映射：

- 标准化映射：是指通过配置映射条件，将第三方日志转换为山石网科设备的标准日志格式，以便在智源平台中展示相应的威胁事件（"第3章 威胁分析" 在第114页>"威胁" 在第115页>"事件列表" 在第136页）。标准化映射的映射条件包括字段名称映射和字段值映射。其中字段映射条件中，威胁名称、源IP/端口、目的IP/端口仅支持字段名称映射。

- 自定义映射：是指通过配置映射条件，将第三方日志转换为用户期望的日志格式，增加日志信息的可读性。自定义映射的映射条件包括字段名称映射、字段名称和值映射两种。

注意:

- 目前，网络威胁日志、主机威胁日志、资产信息日志、常规日志（URL日志、上网行为审计日志、防篡改日志、文件过滤日志、网页安全日志、内容过滤日志）可支持标准化映射和自定义映射，且可以同时配置；除上述7种日志之外的其他类型日志，仅支持自定义映射。其中，资产信息日志仅用于资产识别，解析后不会在Syslog日志页面进行展示。
- 日志标准化配置中均为非必填项，用户可根据需求添加映射条件。

配置日志标准化，请按照以下步骤进行操作：

1. 完成解析流程配置后，点击“下一步”，打开第二步“标准化”配置页面。
2. 点击启用按钮，开启日志标准化功能。



3. 配置标准化映射条件：
   - 在“名称映射”、“源IP/端口映射”、“目的IP/端口映射”条件中，分别点击“源字段名称”下拉菜单，选择上一步解析后的字段名称。
   - 对于威胁日志：在“威胁级别映射”、“威胁类别映射”、“威胁子类别映射”、“动作映射”条件中，指定字段名称映射和字段值映射。
   - 对于常规日志：在“级别映射”、“动作映射”条件中，指定字段名称映射和字段值映射。
   - 点击“源字段名称”下拉菜单，选择上一步解析后的字段名称。

- 在“源字段值”文本框中输入需要映射的源字段值，多个字段值之间用英文逗号隔开；然后点击“映射为”下拉菜单选择源字段值需要映射到的内容。如需添加多个源字段值映射，点击“添加值映射”。例如：威胁级别映射中，指定源字段“High”映射为“严重”，即将High级别的第三方原始威胁日志映射为严重级别的山石网科威胁日志。

4. 在“自定义映射”部分配置自定义映射条件。
   - 点击“源字段名称”下拉菜单，选择上一步解析后的字段名称。
   - 在“源字段值”文本框中输入需要映射的源字段值，多个字段值之间用英文逗号隔开；然后点击“映射为”下拉菜单选择源字段值需要映射到的内容。如需添加多个源字段值映射，点击“添加值映射”。
   - 如需添加多个“字段名称映射条件”或者多个“字段名称和值映射”，点击“添加名称映射”或“添加名称和值映射”。
5. 删除映射条件，点击映射条件最后侧的 ⊖ 按钮。每种类型的映射中，最少要保留一个映射条件。
6. 完成上述标准化配置后，可点击“解析”按钮，打开<解析结果>页面查看威胁日志的字段映射结果。



7. 点击“确定”保存配置。

查看日志解析配置

日志解析配置页面列表中包含预定义日志解析配置以及已创建的自定义日志解析配置。

点击“日志管理 > 日志解析 ”，选择<日志解析配置>标签页，打开日志解析配置页面。



- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的日志解析配置。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击“新配置”，新建自定义日志解析配置。
- 在自定义日志解析配置的“日志解析模板”部分，右上角“名称”文本框中指定名称或在下拉菜单中选择日志类型，筛选列表中的日志解析模板。
- 点击“新模板”，新建日志解析模板。

- 点击列表中指定自定义日志解析配置/日志解析模板的按钮，打开编辑页面，编辑所选日志解析配置/日志解析模板的参数信息。
- 点击列表中指定自定义日志解析配置/日志解析模板的按钮，删除所选自定义日志解析配置/日志解析模板。如需批量删除自定义日志解析配置/日志解析模板，勾选多个自定义日志解析配置/日志解析模板条目，点击页面右上角的“删除”按钮。
- 点击列表中自定义日志解析配置/日志解析模板的名称，打开详情页面，查看自定义日志解析配置/日志解析模板的详细配置信息以及被关联的日志解析规则。在该页面，还可以点击“编辑”按钮，修改自定义日志解析配置/日志解析模板的配置信息。
- 点击页面左下角按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角按钮，刷新日志解析配置页面列表。



注意:

- 系统预定义日志解析配置以及对应日志解析模板，仅可查看，不可以被编辑或删除。
- 被日志解析规则引用的日志解析配置，不可以被删除，如需删除， 必须首先从日志解析规则中删除对该日志解析配置的引用。

配置日志解析规则

日志解析配置以及对应的日志解析模板完成配置后，只有把它引用到日志解析规则中，日志解析功能才能生效。

日志解析规则包括预定义日志解析规则和自定义日志解析规则。系统提供两条预定义日志解析规则：Linux Syslog和山石云鉴Syslog日志解析规则，并默认接收所有主机日志，其中山石云鉴Syslog日志解析规则默认为关闭状态。预定义日志解析规则不可被删除和编辑。

新建自定义日志解析规则

新建自定义日志解析规则，请按照以下步骤进行操作：

1. 选择“日志管理>日志解析”。
2. 选择<日志解析规则>标签页。

3. 点击“新规则”按钮，打开<新日志解析规则>页面。



配置日志解析规则相关信息。

选项	说明
规则状态	点击启用按钮，启用该自定义日志解析规则。
规则配置	
规则名称（必填项）	输入自定义日志解析规则的名称。
接入方式（必填项）	点击下拉菜单，选择日志类型。目前，仅支持选择Syslog类型。
日志解析配置	将日志解析配置引用到日志解析规则中。

选项	说明
（必填项）	点击下拉菜单，勾选已创建完成的日志解析配置，或者直接选择预定义日志解析配置，可多选。
日志源IP	指定需要进行日志解析的日志源设备IP地址。 • 选择“Any”，表示日志解析功能对任意日志源IP地址均生效。 • 选择“自定义”，并在下方文本框中输入日志源IP地址，然后点击“添加”按钮，表示日志解析功能对指定日志源IP地址生效。
描述	输入日志解析规则的描述信息。

4. 点击“确定”按钮，配置完成的自定义日志解析规则将显示在列表中。



注意:

- 系统最多允许创建100条自定义日志解析规则，且最多可同时启用20条自定义日志解析规则。
- 每个日志解析规则最多可以引用3个日志解析配置。
- 请确保日志源IP可以正常发送日志到智源平台，如果该日志源IP未包含在"日志源管理" 在第409页页面的日志源中，将会无法正常完成日志解析功能。
- 同一个日志解析规则在引用的日志解析配置时，不同日志解析配置中的模板不能解析同一种日志格式的日志信息，否则将会出现解析冲突的问题。

查看日志解析规则

日志解析规则页面列表中包含预定义日志解析规则以及已创建的自定义日志解析规则。

点击“日志管理 > 日志解析 ”，选择<日志解析规则>标签页，打开日志解析规则页面。



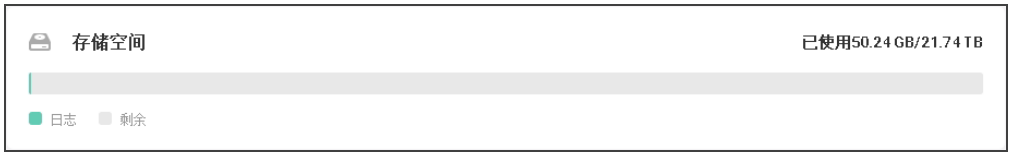
- 点击上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的日志解析规则。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击列表中“状态”栏的按钮，启用或禁用该日志解析规则。表示日志解析规则状态为已启用，表示日志解析规则状态为禁用。
- 点击列表中指定日志解析规则的按钮，打开编辑页面，编辑所选日志解析规则的参数信息。
- 点击列表中指定日志解析规则的 按钮，删除所选日志解析规则。如需批量删除日志解析规则，勾选多个日志解析规则条目，点击页面右上角的“批量删除”按钮。
- 点击“新规则”按钮，新建自定义日志解析规则。
- 点击列表中日志解析规则的名称，打开详情页面，查看日志解析规则的详细配置信息以及被关联的日志解析配置。在该页面，还可以点击“编辑”按钮，修改日志解析规则配置信息。
- 点击页面左下角 按钮，在弹出页面中选择相应视角下的表格展示项。
- 点击页面左下角 按钮，刷新日志解析规则页面列表。

日志存储管理

智源平台可以采集到大量来自于网络设备、流量探针、威胁探针和用户主机的日志信息，同时还可以存储智源平台产生的系统日志信息。用户可以在日志存储管理中查看智源平台的存储空间、备份日志信息以及查看备份日志信息。

查看存储空间

点击“系统设置>日志管理”，选择<日志存储管理>标签页，打开日志存储管理页面。



- 右上角展示智源平台已使用的存储空间大小以及磁盘总空间大小。
- 绿色部分表示设备存储的日志占比。
- 灰色部分表示磁盘剩余空间的占比。

查看日志备份

智源平台支持将备份至FTP服务器的日志信息重新导入到智源平台中进行查看。

导入备份日志

导入备份的日志，请按照以下步骤进行操作：

1. 选择“日志管理”。
2. 选择上方<日志存储管理>标签页，打开日志存储管理页面。
3. 选择下方<查看日志备份>标签页。
4. 在“FTP地址”下拉菜单选择备份日志所在的FTP服务器。具体FTP配置，请参阅FTP配置。
5. 在“日志文件”下拉菜单中，勾选复选框，选择需要导入到智源平台的日志文件。目前系统支持

恢复ZIP格式的日志备份文件。

6. 点击“导入备份”按钮，开始进行导入备份的日志信息。

> **注意:** 智源平台最多可以存储7份已恢复的日志备份文件，且不可重复导入相同的日志文件以及同一天同一类型的日志文件。如果当前已恢复的日志备份文件总数已达到7个，如需继续导入日志，请先删除已恢复的日志备份。

查看已恢复的日志备份

完成导入备份日志后，在下方列表中将显示已恢复的日志备份列表。



- 导入日志备份有以下4种颜色进度条，均表示不同的含义：
  - 蓝色进度条+百分比：表示日志正在导入，以及导入的进度。此时，不可查看该日志备份。
  - 绿色进度条+“√”：表示日志导入成功。可以点击 按钮 查看详细日志信息。
  - 红色进度条+“×”：表示日志导入失败。可能由于日志备份文件不完整或网络问题等原因，导致日志导入失败，不可查看该日志备份。

- 灰色进度条+“时钟”：表示日志等待导入，即当前正在导入的日志还未完成导入，此时，不可查看该日志备份。

- 点击“查看全部”按钮，打开新页面，按照日志类型分类，查看所有已恢复的日志信息。
- 点击日志备份条目后的按钮，删除所选的日志备份。

日志备份配置

智源平台支持对收集的日志信息进行备份。用户可手动或自动将日志信息备份到指定的FTP服务器。

备份文件自动命名，格式为：日志索引名称+日志日期+智源平台SN号+备份文件生成时间。

自动备份

自动备份日志，每天02:00自动将指定类型的日志信息（前一天）备份到指定FTP服务器上。

编辑自动备份计划，请按照以下步骤进行操作：

1. 选择“日志管理”。
2. 选择上方<日志存储管理>标签页，打开日志存储管理页面。
3. 选择下方<日志备份配置>标签页。
4. 点击“自动备份”，然后点击“编辑备份计划”按钮。



在“自动备份”页面，填写自动备份计划配置信息。

选项	说明
自动备份	开启或关闭自动备份日志功能。表示开启，表示关

选项	说明
	闭。
FTP	从下拉菜单中选择已创建的FTP配置，将日志导出到该FTP主机上。用户可根据需要点击“测试”按钮查看该FTP的主机地址是否有效。 具体FTP配置，请参阅FTP配置。
备份周期	自动备份周期默认为每天02:00:00，即每天凌晨2点将会执行自动备份计划。
备份内容	勾选需要备份的日志类型复选框。用户可选择一个或多个日志类型进行备份。

5. 点击“保存”按钮，保存自动备份计划。

手动备份

手动备份日志，手动将指定时间的日志信息备份到指定FTP服务器上。

编辑手动备份计划，请按照以下步骤进行操作：

1. 选择“日志管理”。
2. 选择上方<日志存储管理>标签页，打开日志存储管理页面。
3. 选择下方<日志备份配置>标签页。
4. 点击“手动备份”。



在“手动备份”页面，填写手动备份计划配置信息。

选项	说明
FTP	从下拉菜单中选择已创建的FTP配置，将日志导出到该FTP主机上。用户可根据需要点击“测试”按钮查看该FTP的主机地址是否有效。 具体FTP配置，请参阅FTP配置。
时间	指定需要备份的日志时间周期。 • 开始时间：选择需要备份的日志开始时间。 • 结束时间：选择需要备份的日志结束时间。 • 还可以可直接点击“1天/7天/30天”。 **注意**: • Syslog、Linux类型的日志信息支持备份最近180天的日志。 • NetFlow、MetaData、Sysmon类型的日志信息仅支持备份前一天的日志。 • 可以选择180天范围以内的日志信息，但起止时间跨度不能超过30天。
备份内容	勾选需要备份的日志类型复选框。用户可选择一个或多个日志类型进行备份。

5. 点击“开始备份”按钮开始进行备份。

FTP配置

日志的备份与导入，都通过FTP方式来完成。

新建FTP服务器

新建FTP服务器，请按照以下步骤进行操作：

1. 选择“日志管理”。
2. 选择上方<日志存储管理>标签页，打开日志存储管理页面。
3. 选择下方<FTP配置>标签页。
4. 点击“新FTP”按钮，打开<新FTP>页面。



在“新FTP”页面，填写配置信息。

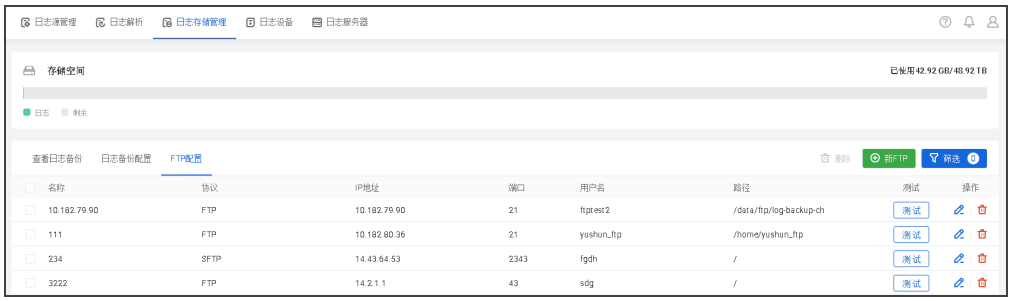
选项	说明
名称（必填项）	输入FTP服务器名称。最多可输入20个字符。
协议	指定FTP服务器使用的协议，可选择FTP或SFTP。
IP地址/端口（必填项）	输入FTP服务器的地址和相应的端口号。地址仅支持IPv4格式。端口号取值范围为0-65535。
用户名（必填项）	登录FTP服务器的用户名。最多可输入20个字符。
密码	指定用户名对应的密码。
路径（必填项）	指定FTP服务器的文件夹路径。此路径对应的文件夹用来存储备份日志，或用来存储需要导入的日志。

5. 配置完成后，点击“测试”按钮测试智源平台与FTP服务器的连通性。用户也可以直接点击“确定”按钮保存此条FTP服务器的配置并返回FTP配置列表。智源平台将不会进行连通性测试。

查看FTP配置列表

FTP配置列表列出已创建的FTP服务器配置信息，包括名称、IP地址、端口号等。

点击“系统设置>日志管理>日志存储管理"，选择“FTP配置”，打开FTP配置列表页面。



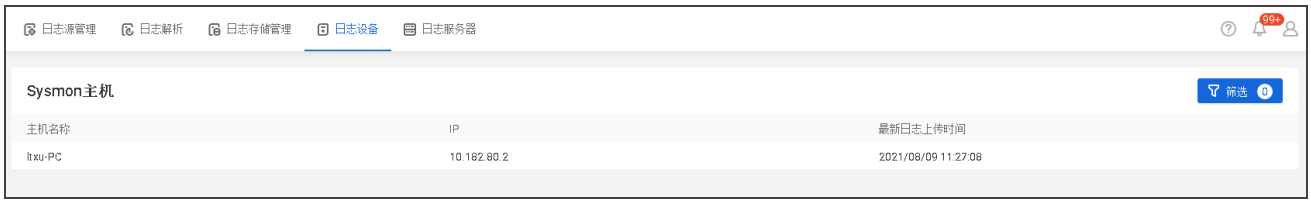
- 在列表中“测试”列，用户可点击“测试”按钮，对FTP服务器进行连通性测试。
- 点击列表中FTP服务器条目后的 按钮，打开“编辑FTP”页面，编辑所选FTP服务器。
- 点击列表中FTP服务器条目后的 按钮，删除所选FTP服务器。如需批量删除FTP服务器，勾选多个FTP服务器条目或者勾选“名称“列复选框进行全选，然后点击“删除”按钮。
- 点击列表上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的服务器信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新FTP列表。

日志设备

智源平台可以收到所有来自装有威胁溯源插件的用户主机的Sysmon日志信息，包含威胁溯源插件采集到的主机进程创建、网络访问、文件操作、注册表修改等相关行为信息。

日志设备页面以列表的形式展示了最近一天内向智源平台发送了Sysmon日志信息的用户主机设备信息，包括主机名称、设备IP地址以及最新上传日志的时间。

点击“日志管理”，选择<日志设备>标签页，打开日志设备页面。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的Sysmon主机。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新Sysmon主机列表。

日志服务器

系统支持将收到的Syslog类型的日志信息、以及智源平台产生的威胁事件转发到日志服务器中。

用户可以在“日志服务器”页面新建、编辑或删除日志服务器。

点击“系统设置>日志管理”，选择<日志服务器>标签页，打开日志服务器页面。



- 列表中“状态”栏显示日志服务器的开启状态。表示启用，表示禁用。
- 点击列表中日志服务器条目后的按钮，打开“编辑日志服务器”页面，编辑所选日志服务器。
- 点击列表中日志服务器条目后的按钮，删除所选日志服务器。如需批量删除日志服务器，勾选多个日志服务器条目，点击上方“删除”按钮。
- 点击“新服务器”按钮，创建日志服务器，详细步骤请参阅新建日志服务器。
- 点击页面左下角按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角按钮，刷新日志服务器列表。

新建日志服务器

新建日志服务器，请按照以下步骤进行操作：

1. 选择“日志管理”。
2. 选择<日志服务器>标签页。

3. 点击“新服务器”按钮，打开“新日志服务器”页面。



在“新日志服务器”页面，填写日志服务器配置信息。

选项	说明
服务器名称/IP（必填项）	指定日志服务器的名称或IP地址。
协议（必填项）	选择日志服务器的协议类型，包括UDP或Secure-TCP。
服务器端口（必填项）	输入日志服务器的协议端口号。
日志类型	选择该日志服务器接收的日志信息的类型。
状态	启用或禁用该日志服务器。

4. 点击“确定”按钮完成配置。

第12章 系统设置

系统设置部分包含如下内容：

- "系统信息" 在第446页：介绍系统基本信息，包括设备序列号、设备名称、硬件平台、系统时间及运行时间、软件版本、规则库版本等。
- "权限设置" 在第448页：介绍如何查看管理员列表以及如何对管理员进行相关配置。
- "联系人管理" 在第454页：介绍如何查看联系人列表以及如何新建联系人。
- "系统日志" 在第457页：介绍如何查看产生的系统事件日志、操作日志。
- "升级管理" 在第461页：介绍如何将系统升级或降级到指定版本。
- "安全设置" 在第462页：介绍如何配置登录策略、密码策略。
- "许可证管理" 在第466页：介绍如何申请、安装许可证以及查看当前系统安装所有许可证。
- "通讯配置" 在第469页：介绍配置邮件服务器，将系统日志等信息发送到指定的邮箱以及短信网关配置。
- "告警通知" 在第471页：如何查看告警通知。
    - "告警通知设置" 在第473页：介绍如何配置自动告警通知规则、威胁告警通知规则和系统告警通知规则。
- "网络管理" 在第492页：介绍如何配置智源平台的IP地址、网关以及DNS服务器。
- "证据信息管理" 在第495页 ： 介绍如何配置证据信息报文存储功能。
- "探针管理" 在第497页：介绍如何查看与智源平台连接的探针的详细信息，包括探针状态、IP地址、序列号、设备型号、实时流量等。
- "级联管理" 在第499页：介绍如何级联智源平台，包括查看以及编辑本级平台、下级平台和上级平台的信息等。
- "集群管理" 在第506页：介绍如何查看智源平台集群中的所有设备的详细信息，以及手动升级从节点的系统版本。

- "安全分析计划" 在第507页：介绍如何将智源平台检测出的威胁事件上报至云景平台。
- "人行数据对接" 在第508页：介绍如何与人民银行金融行业态势感知与信息共享平台进行数据对接。
- "恢复出厂设置/退出/重启/关机" 在第515页：介绍恢复出厂设置、退出系统、重启系统以及关机的相关操作。

系统信息

用户可以在系统信息页面查看基本系统信息，包括设备序列号、设备名称、硬件平台、系统时间及运行时间、软件版本、规则库版本等。

查看系统信息

查看系统信息，选择“系统设置>系统信息”，系统相关信息如下：

选项	说明
系统信息	
序列号	显示该设备的序列号。
激活状态	显示系统是否被激活。
设备名称	显示该设备的名称。点击 按钮，可以修改该设备名称。
硬件平台	显示设备的硬件平台型号。
系统时间	显示该设备的系统日期和时间。点击 按钮，可以修改系统时间。 • 与Internet时间服务器同步：通过与NTP服务器同步的方式配置系统时间。 • 在“服务器1”文本框中指定NTP服务器的IP地址；如果需要，在“服务器2”中指定另一个NTP服务器IP地址。配置第二个NTP服务器后，当系统无法与第一个NTP服务器同步时间时，将尝试与第二个NTP服务器同步。 **注意**：集群部署环境下的智源平台不支持修改系统时间。
软件版本	显示设备当前的软件版本。
下载根证书	点击右上角“下载根证书”按钮，下载根证书。下载完成后，解压已下载的根证书压缩包，然后将根证书导入到本地主机系统中。导入步骤可参考压缩包中的“证书导入帮助文档”。 根证书导入完成后，使用当前主机访问智源平台系统时的连接即

选项	说明
	为安全连接。 **注意**：导入根证书后，需要重新启动浏览器。
系统运行时间	显示系统已运行时长。
情报库信息	
山石域名情报库	显示设备的山石域名情报库当前版本。
山石恶意代码情报库	显示设备的山石恶意代码情报库当前版本。
山石IP情报库	显示设备的山石IP情报库当前版本。
山石弱点情报库	显示设备的山石弱点情报库当前版本。
山石入侵检测特征库	显示设备的山石入侵检测特征库当前版本。
地理库	显示设备的地理库当前版本。

权限设置

用户可以在权限设置页面查看用户列表、对用户以及可信主机进行相关配置。

用户配置

设备的用户根据角色的不同，对系统可执行的管理和配置权限不同。

系统默认预定义如下四类用户角色，这四类用户角色不可被删除和编辑：

- 系统管理员：拥有读、执行和写权限，可以对设备所有功能模块进行配置。
- 系统操作员：拥有读、执行和部分写权限，可以对设备除权限设置和系统日志以外的其他功能模块配置。
- 日志审计员：只可以对设备系统日志模块进行操作，包括查看、导出和配置。
- 系统管理员（只读）：拥有读和部分执行权限，可对设备所有页面进行查看，但是不能配置 。



注意:

- 设备拥有一个默认系统管理员“hillstone”，用户可以对系统管理员“hillstone”进行编辑（除名称之外），但是不能删除该管理员。
- 除了系统管理员，其他角色的用户不能进行权限设置。

新建用户

新建用户，请按照以下步骤进行操作：

1. 选择“系统设置 > 权限设置”，进入到权限配置页面。
2. 选择<用户配置>标签页，打开所有用户列表。

3. 点击“新用户”按钮，弹出<新用户>页面。



在<新用户>页面，配置用户基本信息。

选项	说明
名称	在“名称”文本框中输入用户的名称。
角色	从下拉菜单选择用户的角色。不同的用户角色拥有不同的权限。
部门	在“部门”文本框中输入用户所在的部门。
密码	在“密码”文本框中输入用户的登录密码。密码的设定需符合已设置的密码规则。 关于密码规则的配置（系统设置 > 安全设置>密码策略），请参阅配置密码规则。
确认密码	在“重新输入密码”文本框中再次输入用户密码进行确认。
描述	用户可根据需要指定管理员的描述信息。

4. 点击“确定”按钮保存所做的配置。新创建的用户将会显示在用户列表中。

删除用户

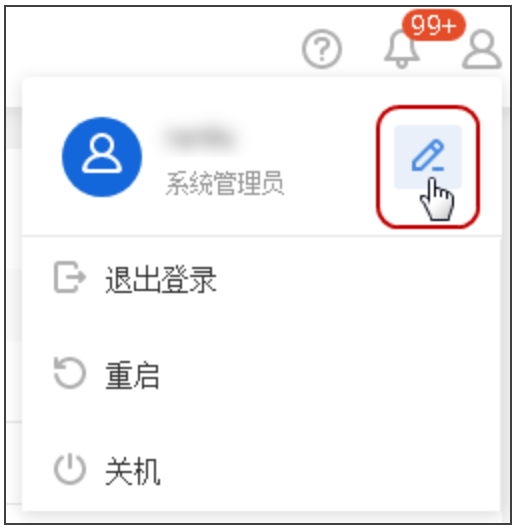
删除用户（仅系统管理员可以操作），请按照以下步骤进行操作：

1. 选择“系统设置 > 权限设置”，进入到权限配置页面。
2. 选择<用户配置>标签页，打开所有用户列表。
3. 在需要删除的用户条目后，点击 按钮，删除该系统管理员/系统操作员/日志审计员/系统管理员（只读）。
4. 如需批量删除用户，勾选多个用户条目，点击页面右上角的“删除”按钮。

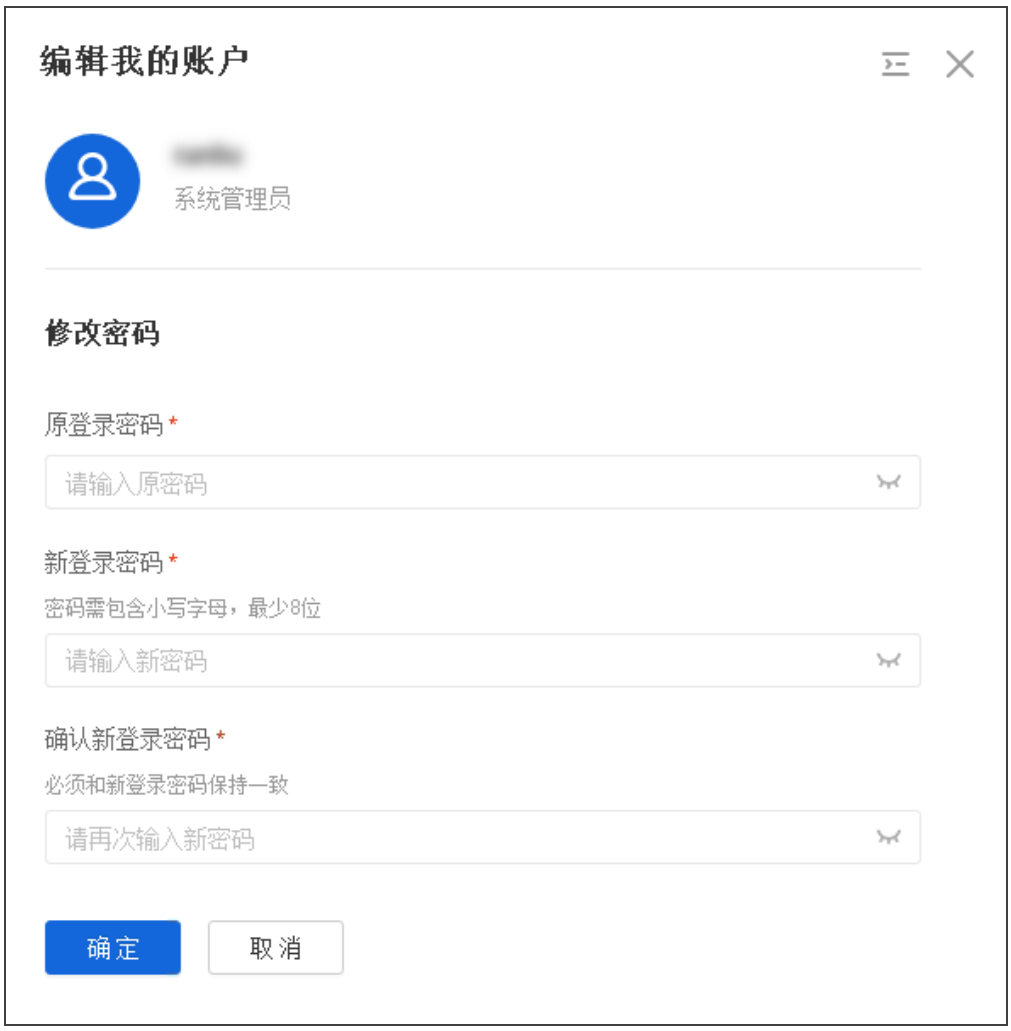
修改用户密码

用户可以在系统页面右上角我的账户中 ，修改用户的登录密码，请按照以下步骤进行操作：

1. 点击系统页面右上角 按钮，然后在弹出框中点击用户名称后的按钮。



2. 在打开的<编辑我的账户>页面中，输入原登录密码、新登录密码以及再次确认新登录密码。



3. 点击“确定”按钮，保存密码配置。

注意: 新登录密码需要符合已设置的密码规则，关于密码规则的配置（系统设置 > 安全设置>密码策略），请参阅配置密码规则。

可信主机

智源平台使用可信主机来进一步保证系统安全。用户可以指定一个IP地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以访问智源平台。

注意: 如果远程主机不能访问智源平台，可能是可信主机配置问题，请进行相关检查。

新建可信主机

新建可信主机，请按照以下步骤进行操作：

1. 选择“系统设置 > 权限设置”，进入到权限配置页面。
2. 选择<可信主机>标签页，打开所有可信主机列表。
3. 点击“新主机”按钮，弹出<新可信主机>页面。



在<添加主机>页面，配置可信主机基本信息。

选项	说明
类型	指定可信主机地址类型，选择“IP地址/掩码”或“IP范围”单选按钮。 • IP地址/掩码：在“IP”文本框中分别输入可信主机的IP地址和子网掩码。 • IP范围：在“IP”文本框中分别输入可信主机的起始IP地址和终止IP地址。

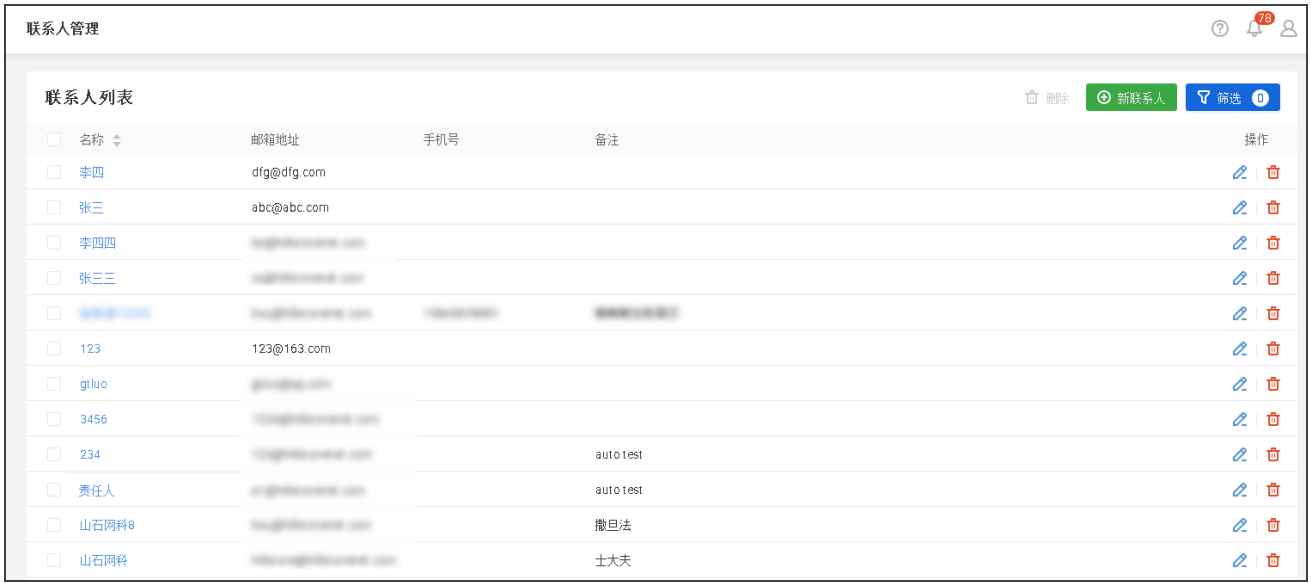
选项	说明
访问权限	启用或禁用该可信主机的访问智源平台的权限。
备注	用户可根据需要指定可信主机的备注信息。

4. 点击“确定”按钮保存所做的配置。新添加的可信主机将会显示在可信主机列表中。

联系人管理

联系人管理页面以列表的方式汇总所有工单处理人、资产责任人以及邮件通知人信息，以便于统一管理。用户可以在工单配置页面、资产配置页面、规则编辑页面、报告任务配置页面中，直接选择已添加的联系人或新增联系人。

点击“系统设置>联系人管理”，打开联系人管理页面。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的联系人。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击联系人名称，打开详情页面，查看所选联系人详细信息。
- 点击列表中联系人条目后的 按钮，打开“编辑联系人”页面，编辑所选联系人。
- 点击列表中联系人条目后的 按钮，删除所选联系人。如需批量删除联系人，勾选多个联系人条目，点击“删除”按钮。
- 点击“新联系人”按钮，创建新的联系人，详细步骤请参阅新建联系人。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新联系人列表。

新建联系人

新增联系人，请按照以下步骤进行操作：

1. 选择“系统设置>联系人管理”。
2. 点击“新联系人”按钮，打开“新联系人”页面。



在“新联系人”页面，填写联系人配置信息

选项	说明
姓名（必填项）	指定联系人的姓名。
电子邮件（必填项）	指定添加的联系人的电子邮箱地址。
手机号码	指定联系人的手机号码。
备注	指定联系人的备注信息。

3. 点击“确定”按钮完成配置。

相关链接：

- "工单管理" 在第281页
- " 第9章 资产管理" 在第337页

- "第10章 引擎管理" 在第384页
- "报告任务" 在第290页

系统日志

设备支持系统日志管理功能。记录并输出智源平台产生的系统事件日志、操作日志。

- 事件日志 - 包括错误、警告、信息、调试4个级别的系统事件信息。
- 操作日志 - 与用户对系统的操作相关的日志信息。

日志的严重等级

系统的事件日志信息根据日志信息的严重程度区分的。系统日志的严重等级可分为4级，关于各级的具体信息，请参阅下表：

级别	描述
错误（Errors）	错误信息。
警告（Warnings）	报警信息。
信息（Informational）	通知信息。
调试（Debugging）	调试信息。

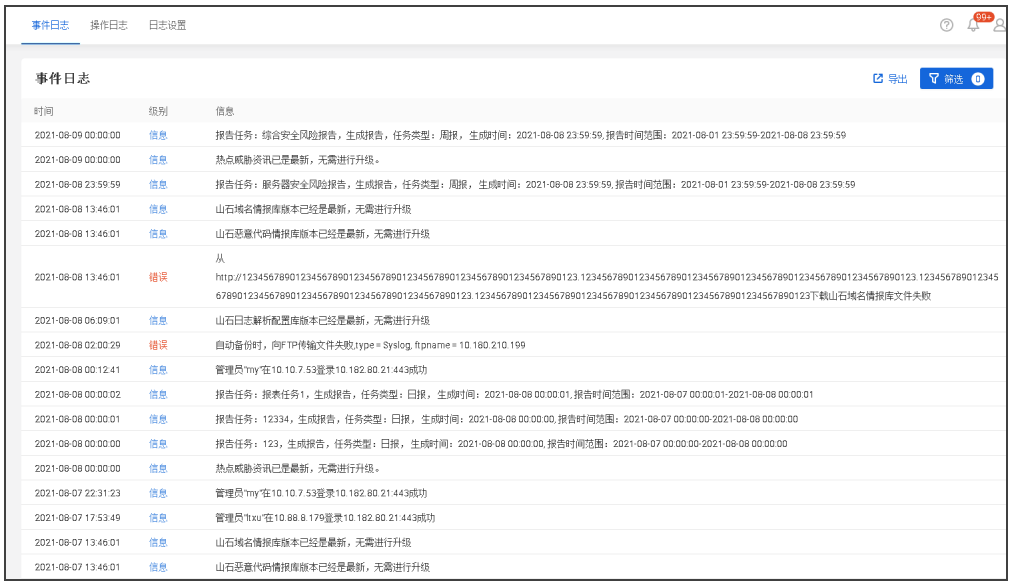
相关链接：

- "事件日志" 在第458页
- "操作日志" 在第459页
- "日志设置" 在第460页

事件日志

用户可以在设备系统日志页面查看、筛选或导出事件日志。

点击“系统设置>系统日志”，再选择“事件日志”标签页，打开事件日志页面。

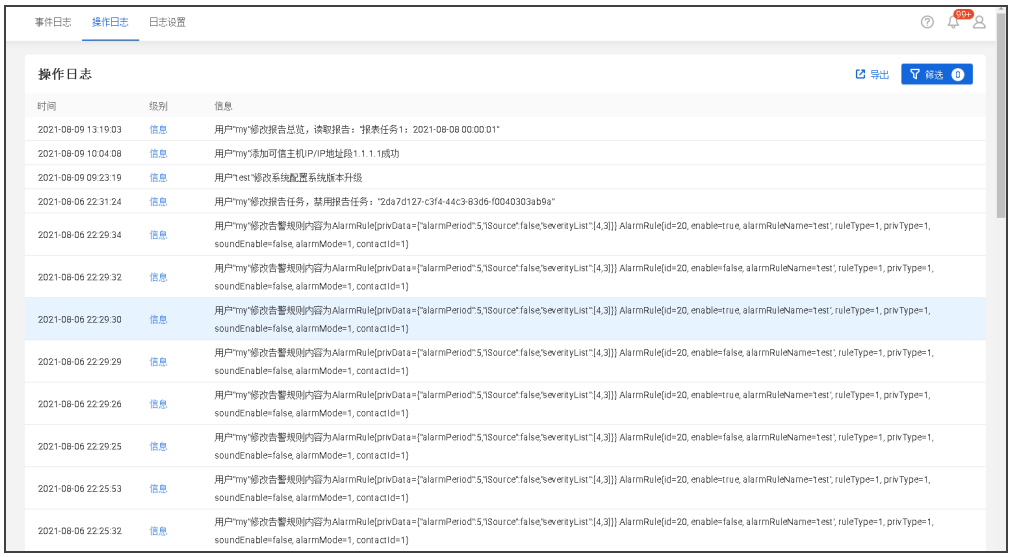


- 点击上方 筛选 0 按钮，然后在弹出部分选择过滤条件，符合过滤条件的日志信息将显示在日志列表中。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击“导出”按钮，以CSV格式导出全部或部分日志条目。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新事件日志页面列表中的日志信息。

操作日志

用户可以在设备系统日志页面查看、筛选或导出操作日志。

点击“系统设置>系统日志”，再选择“操作日志”标签页，打开操作日志页面。



- 点击上方 筛选 0 按钮，然后在弹出部分选择过滤条件，符合过滤条件的日志信息将显示在日志列表中。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击“导出”按钮，以CSV格式导出全部或部分日志条目。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角 按钮，刷新操作日志页面列表中的日志信息。

日志设置

用户可以在日志设置页面配置日志保存相关选项。

点击“系统设置>系统日志”，再选择“日志设置”标签页，打开日志设置页面。



- 点击“编辑”按钮，在“日志最大保存时间”下拉菜单选择时间，指定系统保存日志的最长时间，当超过该指定值后，系统将会删除已保存的日志信息。

升级管理

用户可以在版本升级配置页面将系统升级或降级到指定版本。

系统版本升级

升级软件版本，请按照以下步骤进行操作：

1. 点击“系统设置 > 升级管理”，打开系统版本升级页面。
2. “当前版本”后显示当前系统软件的版本号。
3. 点击“选择文件”按钮，在本地计算机选择离线升级的软件版本文件。
4. 选择文件后，点击“立即升级”按钮，系统开始上传新版本。
5. 上传完成后，系统将会自动重启。

安全设置

用户可以在安全设置页面配置用户登录策略、登录密码策略、密码周期策略等。

登录策略

系统管理员可以指定登录超时时间以及登录失败后的用户锁定配置。



登录超时

开启登录超时功能后，当用户登录设备后，如果在指定的超时时间结束时未执行任何操作，再次执行操作时则需要重新登录设备。默认情况下，登录超时功能为启用状态，且默认超时时间为60分钟。

配置登录超时功能，请按照以下步骤进行操作：

1. 点击“系统设置 > 安全设置”，打开“安全设置”页面。
2. 在“登录策略”部分，点击“登录超时”下方启用按钮，可开启/关闭登录超时功能。
3. 在文本框中输入超时时间，单位为分钟，范围是1-1440分钟，默认值为60分钟。
4. 点击右上角“保存”按钮。
5. 如需恢复默认配置，点击右上角“恢复默认”按钮。

用户锁定

开启用户锁定功能并配置锁定限制后，若用户连续输错指定次数的用户名和密码或者同一用户连续输错指定次数的密码，系统将会按照指定的锁定时间锁定该用户账号或IP地址。默认情况下，该功能为启用状态，且在用户使用错误密码尝试5次后，该用户账号将会被锁定3分钟。

配置用户锁定功能，请按照以下步骤进行操作：

1. 点击“系统设置 > 安全设置”，打开“安全设置”页面。
2. 在“登录策略”部分，点击“用户锁定”下方启用按钮，可开启/关闭用户锁定功能。
3. 在“密码尝试次数”文本框中输入登录失败次数，范围是1-100次，默认值为5次。
4. 在“锁定时长”文本框中输入锁定时间，范围是1-1440分钟，默认值为3分钟。
5. 勾选“锁定账号”或者“锁定IP”复选框，指定用户的锁定方式。默认为锁定账号。
6. 点击右上角“保存”按钮。
7. 如需恢复默认配置，点击右上角“恢复默认”按钮。

密码策略

系统管理员可以指定用户的密码规则、开启新用户强制修改密码功能以及配置密码强制修改周期。



配置密码规则

指定用户设置密码需符合的密码规则，请按照以下步骤进行操作：

1. 点击“系统设置 > 安全设置”，打开“安全设置”页面。
2. 在“密码策略”部分的“密码最小长度”文本框中指定允许配置的密码的最小长度，范围是4-32位，默认值为8位。
3. 在“密码强度”选项部分勾选密码必须包含的限制条件，包括大写字母、小写字母、数字以及特殊符号，可多选，默认全选所有。
4. 点击右上角“保存”按钮。
5. 如需恢复默认配置，点击右上角“恢复默认”按钮。

开启/关闭新用户强制修改密码

开启新用户强制修改密码功能后，未修改过密码的新用户初次登录设备时，系统将强制该用户修改密码。默认情况下，该功能为关闭状态。

开启新用户强制修改密码功能，请按照以下步骤进行操作：

1. 点击“系统设置 > 安全设置”，打开“安全设置”页面。
2. 在“密码策略”部分，点击“新用户强制修改密码”下方启用按钮，可开启/关闭新用户强制修改密码功能。



注意: 在未开启新用户强制修改密码功能时，如下几种情况下，系统依然会强制修改密码：

- 默认系统管理员“hillstone”使用初始密码首次登录设备时；
- 当系统升级至V2.0R4版本前，系统中的原有用户在升级至V2.0R4版本后首次登录设备时。

配置密码强制修改周期

开启密码强制修改功能后，若用户的账号密码超过指定的使用期限后，系统将在该用户再次登录时强制其用该密码。默认情况下，该功能为关闭状态。

配置密码强制修改周期功能，请按照一下步骤进行操作：

1. 点击“系统设置 > 安全设置”，打开“安全设置”页面。
2. 在“密码策略 ”部分，点击“密码强制修改周期”下方启用按钮，可开启/关闭密码强制修改功能。
3. 在“密码使用期限”文本框中输入限制天数，范围是7-365天，默认值是60天。

密码过期告警

开启密码强制修改功能后，当用户在密码过期前一周内首次登录设备时，系统将会在页面右上角“告警通知”处 

显示告警通知提示，可点击“修改密码”立即修改用户密码，同时在“系统告警通知”内也会加入密码过期告警通知。



许可证管理

许可证（license）用来授权用户使用一些功能、服务，或者用来扩展性能。

对于智源平台的平台许可证，说明如下：

- 如果没有申请和安装平台许可证，智源平台可以正常使用，但是无法连接流量探针设备以及不能升级系统版本；
- 如果已经安装了平台许可证，智源平台可以正常使用并升级系统版本，但最多可以连接20个流量探针设备；
- 如果已经安装的平台许可证到期后，智源平台仍旧可以正常使用，已经连接的流量探针设备也可继续使用，但是无法连接新的流量探针设备以及不能升级系统版本。

许可证展示

选择“系统设置 > 许可证管理”，进入许可证页面。许可证列表部分显示当前系统安装所有许可证。

如果许可证即将过期（有效时间剩余30天内）或者已经过期：

- 登录设备后，在系统“消息”列表中提示许可证即将过期或者已经过期。

申请许可证

安装许可证之前，用户需要先申请许可证请求，请按照以下步骤进行操作：

1. 点击“系统设置 > 许可证管理”，进入许可证页面。
2. 在“许可证列表”右上角点击“申请许可证”按钮，或者点击“许可证申请”标签页，跳转到“许可证申请”页面，

3. 在“许可证申请”页面中，填写生成许可证请求所需要的信息。



4. 点击“确定”，将会出现一串许可证请求码。

5. 复制生成的请求码，发送给销售人员，由其获取许可证再返回给您。

安装许可证

获得许可证后，用户需要将其装载到设备上使其生效。安装许可证，请按照以下步骤进行操作：

1. 选择“系统设置 > 许可证管理”，进入许可证页面。

2. **在<许可证安装>标签页，选择以下两种方式中的一种导入许可证。**



- 输入字符串：选中“输入字符串”单选按钮，然后将许可证字符串内容输入到对应的文本框。

- 上传文件：选中“上传文件”单选按钮，点击“上传文件”按钮，并且选中许可证文件（许可证为.license文件）。

3. 点击“确定”按钮，完成许可证的安装。不需要重启设备，许可证即可生效。

通讯配置

通讯配置包括邮件服务器配置和短信网关配置。

邮件服务器

用户可以在邮件服务器配置页面配置邮件服务器，将系统日志、告警通知等信息发送到指定的邮箱。

新建邮件服务器

新建邮件服务器，请按照以下步骤进行操作：

1. 点击“系统设置 > 通讯配置”，选择<邮件服务器>标签页，进入“邮件服务器”页面。
2. 点击“编辑” 按钮。



在“邮件服务器”页面，填写邮件服务器基本配置信息。

选项	说明
邮件服务器	在文本框输入邮件服务器的域名。
SSL加密	勾选“SSL加密”复选框，邮件使用SSL加密方式和指定端口发送。默认端口号为465。若不勾选，邮件使用普通方式和固定端口25发送。
邮箱账号	在文本框输入发件人的邮箱账号。
邮箱密码	指定邮箱账号对应的授权码。
测试收件人	指定用于测试的账号。点击“测试”按钮，测试配置的邮箱账号是否能够成功发送邮件。该配置项仅用于测试，不

选项	说明
	会被保存。

3. 点击“确定”按钮，保存当前页面所做配置。

短信网关

当产生威胁/系统告警通知时，系统支持发送告警通知短信给指定的收件人，在开启短信通知功能前，用户需要先配置短信网关相关信息。

目前，系统仅支持使用阿里云短信服务网关。

配置短信网关

配置阿里云短信网关，请按照以下步骤进行操作：

1. 点击“系统设置 > 通讯配置”，选择<短信网关>标签页，进入“短信网关”页面。

2. 点击“编辑”按钮。



在“短信网关”页面，填写阿里云短信网关基本配置信息。

选项	说明
Access Key ID	输入阿里云短信服务平台中申请的Access Key ID，作为山石网科设备和阿里云短信服务平台之间相互认证时的用户名。该参数需与在阿里云短信服务平台中申请的模板Access Key ID保持一致。

选项	说明
Access Key Secret	输入阿里云短信服务平台中申请的Access Key Secret，作为山石网科设备和阿里云短信服务平台之间相互认证时的密码。该参数需与在阿里云短信服务平台中申请的模板Access Key Secret保持一致。
短信签名	输入阿里云短信服务平台中申请的短信签名。
威胁告警短信模块Code	复制下方威胁告警短信模板内容至阿里云短信服务平台，用于申请模板Code，审核通过后将返回的威胁告警短信模板Code填写至下方的文本框中。
系统告警短信模块Code	复制下方系统告警短信模板内容至阿里云短信服务平台，用于申请模板Code，审核通过后将返回的系统告警短信模板Code填写至下方的文本框中。
测试手机号码	指定测试手机号码。点击“测试”按钮测试配置的手机号码是否能够成功接收到短信通知。

3. 点击“确定”按钮，保存当前页面所做配置。
4. 点击“清空数据”按钮，清空当前页面的所有配置。

告警通知

系统支持告警通知功能，根据已配置的告警通知设置，对各种类型的威胁事件进行检测，以及对智源平台、流量探针、威胁探针设备状态和系统参数进行检测，当满足告警通知规则的触发条件时，系统将会产生告警信息。同时， 系统还可以通过电子邮件、短信或声音提醒的方式将告警信息及时通知到用户，用户即可针对告警内容实施后续的响应处理。

告警通知信息分为以下4种类型：

- 自动告警通知：与关注资产相关的告警通知信息。添加关注资产后，自动生成告警规则。当关注的资产上发生了符合规则的威胁事件时，将会产生对应的自动告警通知信息。
- 威胁告警通知：与威胁事件相关的告警通知信息。当满足威胁告警通知规则的所有触发条件时，将会产生对应的威胁告警通知信息。

- 系统告警通知：与智源平台、威胁探针、流量探针设备状态和系统参数（CPU利用率、内存利用率和硬盘利用率）相关的告警通知信息。例如：当智源平台状态发生了异常时，将会产生系统告警通知信息。
- 许可证过期：许可证过期通知消息。如果许可证即将过期（有效时间剩余30天内）或者已经过期，将会产生许可证过期告警信息。

相关链接：

- "告警通知设置" 在第473页
- "许可证管理" 在第466页

告警通知设置

告警通知设置，即为配置告警通知规则，规定了告警信息的触发条件以及告警方式，按照类别分为自动告警通知规则、威胁告警通知规则和系统告警通知规则。

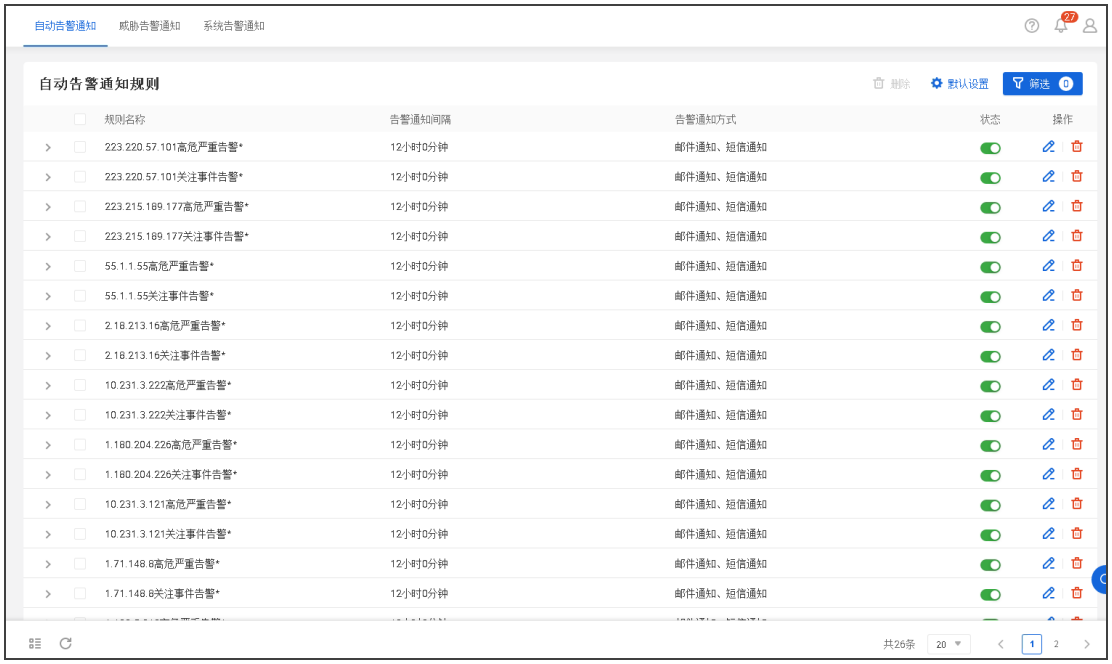
- 自动告警通知规则：用户需要重点关注某些资产时，可以将该资产添加为关注，此时系统会自动生成告警规则。当关注的资产上发生了符合规则的威胁事件时，系统将会产生一条告警信息，并按照规则中指定的告警方式（邮件通知、短信通知、声音提醒）及时通知到用户。
- 威胁告警通知规则：在用户需要重点关注某些威胁事件时，可以按照这些威胁事件新建威胁告警通知规则。当符合所有威胁告警通知规则触发条件的威胁事件发生时，系统将会产生一条告警信息，并按照规则中指定的告警方式（邮件通知、短信通知、声音提醒）及时通知到用户。
- 系统告警通知规则：在用户需要关注智源平台、威胁探针、流量探针设备状态和系统参数时，可以新建系统告警通知规则。当设备状态、CPU利用率、内存利用率和硬盘利用率符合触发条件时，系统将会产生一条告警信息，并按照规则中指定的告警方式（邮件通知、短信通知、声音提醒）及时通知到用户。例如：流量探针的上下线状态告警提醒、智源平台的状态异常告警提醒。

用户可以在告警设置页面查看已有的告警通知规则，编辑自动告警通知规则以及新建威胁告警通知规则和系统告警通知规则。

查看告警通知规则

告警通知规则列表中展示所有已有的告警通知规则。

点击“系统设置 > 告警通知设置 ”，选择<自动告警通知>、<威胁告警通知>或<系统告警通知>标签页，打开告警通知规则页面。



- 点击列表上方 筛选 0 按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的规则。圆圈中的数字表示已配置筛选条件的个数，点击“重置”按钮，删除已经添加的筛选条件。
- 点击告警通知规则名称前 > 按钮，展开告警通知规则详细配置信息。
- 点击列表中“状态”栏的 按钮，启用或禁用该告警通知规则。 表示告警通知规则状态为已启用， 表示告警通知规则状态为禁用。
- 点击<自动告警规则>列表右上角“默认设置”按钮，编辑自动告警通知规则的默认设置。
- 点击列表中指定告警通知规则的 按钮，打开编辑页面，编辑所选告警通知规则的配置信息。
- 点击规则列表中“操作”列的 按钮，在弹出的对话框中点击“确定”，删除所选规则。如需批量删除规则，勾选多个规则条目或者勾选“名称“列复选框进行全选，然后点击页面右上角的“删除”按钮。
- 点击页面左下角 按钮，在弹出页面中勾选需要显示的列名称
- 点击页面左下角 按钮，刷新告警通知规则页面列表。

注意: 若重点关注资产被删除或取消关注，则会将关于该条资产的自动告警规则删除。

编辑自动告警通知规则

系统支持编辑自动告警通知规则的默认设置统一修改所有规则的配置，或者单独编辑指定规则的配置。

默认设置

默认告警规则包括“关注事件告警规则”和“严重高危事件告警规则”两种。在页面右上方点击“启用”按钮，可同时启用/禁用两种默认告警规则，默认情况下为启用状态，用户将资产设置为重点关注资产后，系统将按照当前的默认配置自动生成两条关于该资产的告警规则。若禁用默认告警规则，则不会生成关于重点关注资产的全新告警。

关注事件告警规则

当重点关注资产上发生了被关注的威胁事件时系统会产生告警，配置相关规则，请按照以下步骤进行操作:

1. 选择“系统设置 > 告警通知设置”，进入到告警通知设置页面。
2. 在<自动告警通知>标签页，点击“默认设置”，进入<默认告警规则>页面。
3. 在<默认告警规则>页面，点击<关注事件告警规则>标签页。



在<关注事件告警规则>标签页，配置相关信息。

选项	说明
规则状态	点击启用按钮，启用或禁用告警通知规则。默认情况下为启用状态。
告警通知事件	对关注的威胁事件进行告警通知，不可修改。
级别	指定产生自动告警通知需要匹配的威胁事件的级别。点击下拉菜单，勾选威胁级别复选框，可多选。如不指定该参数，则默认为全部。
攻击阶段	指定产生自动告警通知需要匹配的威胁事件的攻击阶段。点击下拉菜单，勾选攻击阶段复选框，可多选。如不指定该参数，则默认为全部。
告警通知间隔	指定产生自动告警通知的时间间隔。默认为12小时。
告警通知方式	指定告警信息的通知方式。默认使用“邮件通知”和“短信通知”两种方式。 • 邮件通知：勾选复选框，开启邮件通知功能。开启后，当产生自动告警通知时，系统会发送告警邮件给指定的收件人。 • 短信通知：勾选复选框，开启短信通知功能。开启后，当产生自动告警通知时，系统会发送告警通知短信给指定的收件人。 • 声音提醒：勾选复选框，开启告警声音提醒功能。开启后，当产生新的自动告警通知或者存在未查看的自动告警通知时，系统将会使用声音提醒用户；或者存在未查看的自动告警通知时，系统将在用户登录智源平台时使用声音提醒用户。同时，自动告警信息将会在告警通知页面显示。关于查看告警通知信息，请参阅"告警通知" 在第471页。 **注意**：如需使用“邮件通知”或“短信通知”功能，请提前配置完成邮件服务器短信网关，请参阅"通讯配置" 在第469页。

4. 点击“确定”，保存配置。

高危严重事件告警规则

当重点关注资产上发生了高危、严重的威胁事件时系统会产生告警，配置相关规则，请按照以下步骤进行操作：

1. 选择“系统设置 > 告警通知设置”，进入到告警通知设置页面。
2. 在<自动告警通知>标签页，点击“默认设置”，进入<默认告警规则>页面。
3. 在<默认告警规则>页面，点击<高危严重事件告警规则>标签页。



在<高危严重事件告警规则>页面，配置相关信息。

选项	说明
规则状态	点击启用按钮，启用或禁用告警通知规则。默认情况下为启用状态。
告警通知事件	指定产生自动告警通知需要匹配的威胁事件的类型。点击下拉菜单，勾选检测的威胁事件类型，可多选。如不指定该参数，则默认为全部。
级别	指定产生自动告警通知需要匹配的威胁事件的级别。点击下拉菜单，勾选威胁级别复选框，可多选。如不指定该参数，则默认选中“高危”和“严重”。
攻击阶段	指定产生自动告警通知需要匹配的威胁事件的攻击阶段。点击下拉菜单，勾选攻击阶段复选框，可多选。如不指定该参数，则默认为全部。
威胁名称包含字段	指定产生自动告警通知需要匹配的威胁事件名称包含的内容。例如：CVE-1999-0067。默认为空，且仅支持配置一个包含内容。
告警通知间隔	指定产生自动告警通知的时间间隔。默认为12小时。
告警通知方式	指定告警信息的通知方式。默认使用“邮件通知”和“短信通知”两种方式。 • 邮件通知：勾选复选框，开启邮件通知功能。开启后，当产生自动告警通知时，系统会发送告警邮件给指定的收件人。 • 短信通知：勾选复选框，开启短信通知功能。开启后，当产生自动告警通知时，系统会发送告警通知短信给指定的收件人。 • 声音提醒：勾选复选框，开启告警声音提醒功能。开启后，当产生新的自动告警通知或者存在未查看的自动告警通知时，系统将会使用声音提醒用户；或者存在未查看的自动告警通知时，系统将在用户登录智源平台时使

选项	说明
	用声音提醒用户。同时，自动告警信息将会在告警通知页面显示。关于查看告警通知信息，请参阅"告警通知" 在第471页。 **注意**：如需使用“邮件通知”或“短信通知”功能，请提前配置完成邮件服务器短信网关，请参阅"通讯配置" 在第469页。

4. 点击“确定”，保存配置。

编辑自动告警通知规则

编辑单条告警规则的配置信息，请按照以下步骤进行操作：

1. 选择“系统设置 > 告警通知设置”，进入到告警通知设置页面。
2. 在<自动告警通知>页面，点击告警规则条目后的按钮，弹出<编辑自动告警通知规则>对话框。



在<编辑自动告警通知规则>页面，配置相关信息。

选项	说明
规则状态	点击启用按钮，启用或禁用告警通知规则。
名称	展示告警通知规则的名称，命名方式为“资产IP+关注事件

选项	说明
	告警*/高危严重告警*” 不可修改。
告警通知事件	产生自动告警通知需要匹配的威胁事件的类型。 • 若是关注事件告警类型的规则，则匹配的威胁事件为用户关注的威胁事件，不可修改。 • 若是高危严重告警类型的规则，点击下拉菜单，勾选检测的威胁事件类型，可多选。如不指定该参数，则默认为全部。
级别	指定产生自动告警通知需要匹配的威胁事件的级别。点击下拉菜单，勾选威胁级别复选框，可多选。如不指定该参数，则默认为全部。
攻击阶段	指定产生自动告警通知需要匹配的威胁事件的攻击阶段。点击下拉菜单，勾选攻击阶段复选框，可多选。如不指定该参数，则默认为全部。
威胁名称包含字段	指定产生自动告警通知需要匹配的威胁事件名称包含的内容。例如：CVE-1999-0067。默认为空，且仅支持配置一个包含内容。
IP	生成该条自动告警规则的重点关注资产的IP地址。
告警通知间隔	指定产生自动告警通知的时间间隔。
告警通知方式	指定告警信息的通知方式。 • 邮件通知：勾选复选框，开启邮件通知功能，并点击下拉菜单选择已配置的联系人作为邮件收件人。开启后，当产生自动告警通知时，系统将会按照配置，发送告警邮件给指定的收件人。关于联系人配置，请参阅"联系人管理" 在第454页。 • 短信通知：勾选复选框，开启短信通知功能，并点击下拉菜单选择已配置的联系人作为短信通知收件人。开启后，当产生自动告警通知时，系统将会按照配

选项	说明
	置，发送告警通知短信给指定的收件人。关于联系人配置，请参阅"联系人管理" 在第454页。 • 声音提醒：勾选复选框，开启告警声音提醒功能。开启后，当产生新的自动告警通知或者存在未查看的自动告警通知时，系统将会使用声音提醒用户；或者存在未查看的自动告警通知时，系统将在用户登录智源平台时使用声音提醒用户。同时，威胁告警信息将会在告警通知页面显示。关于查看告警通知信息，请参阅"告警通知" 在第471页。 **注意**：如需使用“邮件通知”或“短信通知”功能，请提前配置完成邮件服务器短信网关，请参阅"通讯配置" 在第469页。

3. 点击“确定”，保存配置。

新建威胁告警通知规则

新建威胁告警通知规则，请按照以下步骤进行操作：

1. 选择“系统设置 > 告警通知设置”，进入到告警通知设置页面。
2. 选择<威胁告警通知>标签页，打开所有已创建的威胁告警通知规则列表。

3. 点击“新告警规则”按钮，打开<新增威胁告警通知规则>页面。



在<新增威胁告警通知规则>页面，填写威胁告警通知规则配置信息。

选项	说明
规则状态	点击启用按钮，启用或禁用威胁告警通知规则。
名称（必填项）	指定告警通知规则的名称， 范围为1至128个字符。
告警通知事件	指定产生威胁告警通知需要匹配的威胁事件的类型。点击下拉菜单，勾选检测的威胁事件类型，可多选。如不指定该参数，则默认为全部。
级别	指定产生威胁告警通知需要匹配的威胁事件的级别。点击下拉菜单，勾选威胁级别复选框，可多选。如不指定该参数，则默认为全部。
攻击阶段	指定产生威胁告警通知需要匹配的威胁事件的攻击阶段。点击下拉菜单，勾选攻击阶段复选框，可多选。如不指定该参数，则默认为全部。
来源	指定产生威胁告警通知需要匹配的威胁事件的来源，例如：智源平台、威胁探针。点击下拉菜单，勾选来源设备复选框，可多选。如不指定该参数，则默认为全部。
威胁名称包含字段	指定产生威胁告警通知需要匹配的威胁事件名称包含的内容。例如：CVE-1999-0067。仅支持配置一个包含内容。
IP	指定产生威胁告警通知需要匹配的资产的IP地址（可配置为源IP或者目的IP）。 1. 点击下拉菜单，在打开的页面中选择“Any”或“自定义”。“Any”表示威胁告警规则对任意IP地址均生效。 2. 如果选择“自定义”，点击下拉菜单选择“IP掩码”或“IP范围”，并在下方文本框中输入相应的IP地址配置。 3. 点击“添加”按钮，将指定的IP地址/IP地址范围添加到下方。系统最多允许添加8个IP地址/IP地址范围。 如需

选项	说明
	删除已添加的IP地址，点击IP地址后的“×”按钮。
源IP	指定产生威胁告警通知需要匹配的威胁事件的源IP地址。添加方法步骤同上。可指定为IPv6地址。
目的IP	指定产生威胁告警通知需要匹配的威胁事件的目的IP地址。添加方法步骤同上。可指定为IPv6地址。
告警通知间隔	指定产生威胁告警通知的时间间隔。
告警通知方式	指定告警信息的通知方式。 • 邮件通知：勾选复选框，开启邮件通知功能，并点击下拉菜单选择已配置的联系人作为邮件收件人。开启后，当产生威胁告警通知时，系统将会按照配置，发送告警邮件给指定的收件人。关于联系人配置，请参阅"联系人管理" 在第454页。 • 短信通知：勾选复选框，开启短信通知功能，并点击下拉菜单选择已配置的联系人作为短信通知收件人。开启后，当产生威胁告警通知时，系统将会按照配置，发送告警通知短信给指定的收件人。关于联系人配置，请参阅"联系人管理" 在第454页。 • 声音提醒：勾选复选框，开启告警声音提醒功能。开启后，当产生新的威胁告警通知或者存在未查看的威胁告警通知时，系统将会使用声音提醒用户；或者存在未查看的威胁告警通知时，系统将在用户登录智源平台时使用声音提醒用户。同时，威胁告警信息将会在告警通知页面显示。关于查看告警通知信息，请参阅"告警通知" 在第471页。 **注意**：如需使用“邮件通知”或“短信通知”功能，请提前配置完成邮件服务器短信网关，请参阅"通讯配置" 在第469页。

新建系统告警通知规则

新建系统告警通知规则，请按照以下步骤进行操作：

1. 选择“系统设置 > 告警通知设置”，进入到告警通知设置页面。
2. 选择<系统告警通知>标签页，打开所有已创建的系统告警通知规则列表。

3. 点击“新告警规则”按钮，打开<新增系统告警通知规则>页面。



在<新增系统告警通知规则>页面，填写系统告警通知规则配置信息。

选项	说明
规则状态	点击启用按钮，启用或禁用系统告警通知规则。
名称（必填	指定告警通知规则的名称， 范围为1至128个字符。

选项	说明
项）	
设备类型	指定检测的设备类型，包括智源平台、威胁探针或流量探针。
触发条件	
集群节点状态	当设备类型指定为“山石网科智源平台”时，可指定产生系统告警通知需要匹配的设备节点状态。勾选“异常”复选框，当设备节点发生异常时，产生系统告警通知规则。
匹配威胁探针	当设备类型指定为“威胁探针”时，点击下拉菜单勾选系统告警通知规则对应的威胁探针复选框，可多选。
匹配流量探针	当设备类型指定为“流量探针”时，点击下拉菜单勾选系统告警通知规则对应的流量探针复选框，可多选。
探针状态	勾选“离线”或“上线”复选框，当指定的威胁探针/流量探针状态为离线或下线时，将会产生系统告警信息。
系统参数	指定产生系统告警通知需要匹配的系统参数， 包括监测对象和阈值。 勾选“CPU利用率”、“内存利用率”或“硬盘利用率”复选框作为监测对象，然后指定对应阈值。
告警方式	
告警方式	指定告警通知信息的通知方式。 • 邮件通知：勾选复选框，开启邮件通知功能，并点击下拉菜单选择已配置的联系人作为邮件收件人。开启后，当产生系统告警通知时，系统将会按照配置，发送告警通知邮件给指定的收件人。关于联系人配置，请参阅" 联系人管理" 在第454页。 • 短信通知：勾选复选框，开启短信通知功能，并点击下拉菜单选择已配置的联系人作为短信通知收件人。开启后，当产生系统告警通知通知时，系统将会按照配置，发送告警通知短信给指定的收件人。关于联系人配置，

选项	说明
	请参阅"联系人管理" 在第454页。 • 声音提醒：勾选复选框，开启告警声音提醒功能。开启后，当产生新的系统告警通知或者存在未查看的系统告警通知时，系统将会使用声音提醒用户；或者存在未查看的系统告警通知时，系统将在用户登录智源平台时使用声音提醒用户。同时，系统告警信息将会在告警通知页面显示。关于查看告警通知信息，请参阅"告警通知" 在第471页。 **注意**：如需使用“邮件通知”或“短信通知”功能，请提前配置完成邮件服务器短信网关，请参阅"通讯配置" 在第469页。

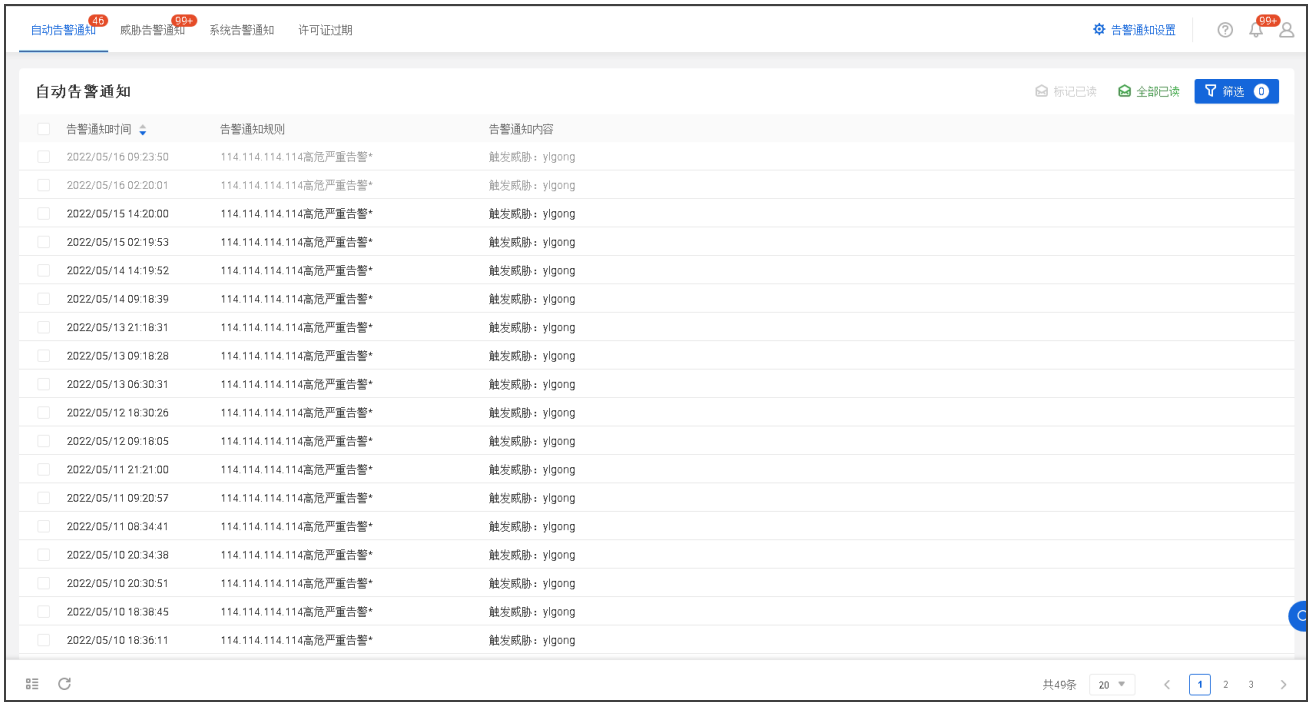
查看告警通知

查看告警通知信息

告警通知页面以列表的形式展示了自动告警通知、威胁告警通知、系统告警通知，包括告警通知时间、对应的告警通知规则和告警通知内容。

点击页面右上角 

按钮，打开告警通知信息页面，分别点击<自动告警通知>、<威胁告警通知>、<系统告警通知>标签页，打开对应的告警通知信息列表页面。



- 标签页右上角数字表示未读告警通知信息的个数。
- 已读告警通知信息在列表中将显示为灰色。如果需要将告警通知信息设置为已读状态，点击告警通知信息条目或者勾选告警通知信息复选框，点击右上角“标记已读”按钮。如需批量标记所有告警通知信息为已读状态，点击页面右上角的“全部已读”按钮。

- 点击列表上方 

按钮，然后在弹出部分指定筛选条件，系统将根据筛选条件筛选特定的告警通知信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新告警通知信息列表。
- 点击“告警设置”跳转至"告警通知设置" 在第473页页，可配置需要的告警通知规则。

查看许可证过期信息

点击页面右上角 

按钮，打开告警通知信息页面，点击<许可证过期>标签页，打开许可证过期通知信息列表页面。

- 已读许可证过期通知信息在列表中将显示为灰色。如果需要将许可证过期通知信息设置为已读状态，点击许可证过期通知信息条目或者勾选许可证过期通知信息复选框，点击右上角“标记已读”按钮。
- 点击页面左下角  按钮，在弹出页面中勾选需要显示的列名称。
- 点击页面左下角  按钮，刷新许可证过期通知信息列表。

网络管理

网络管理用来配置智源平台的IP地址、网关以及DNS服务器。用户可以通过配置的IP访问智源安全运营平台以及连接探针设备。

接口配置

智源平台支持配置不同接口的IP和掩码，以实现通过多个网段访问、管理设备和收发数据的目的。

点击“系统配置 > 网络管理”，进入<接口配置>标签页。

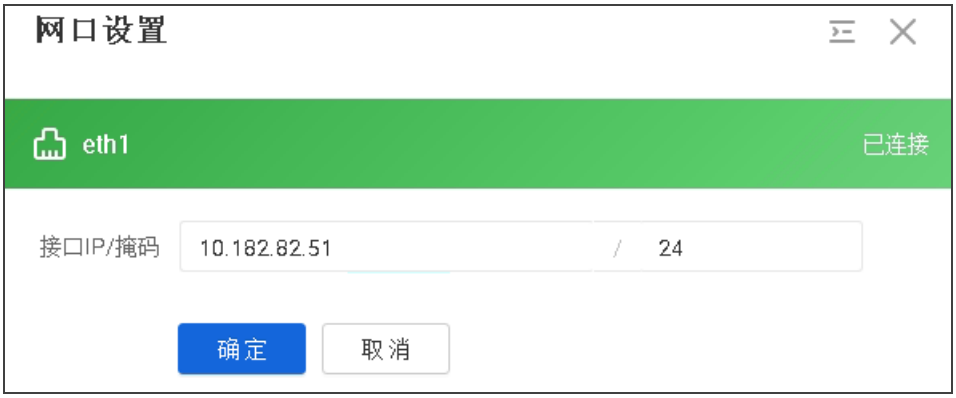


- 展示不同接口IP、接口掩码以及接口的连接状态。接口图标为时表示接口已连接，接口图标为时表示接口未连接。
- 点击按钮，编辑接口的IP以及掩码。具体配置，请参阅编辑接口信息部分。

编辑接口信息

编辑指定接口的IP和掩码，请按照以下步骤进行操作：

1. 点击“系统设置 > 网络管理”，打开<网络管理>页面。
2. 选择接口，点击按钮，打开<网口设置>页面。



在“网络管理”页面，填写网络相关参数。

选项	说明
接口IP	在部署智源平台时，可通过CLI配置接口IP地址。如需修改，在“接口IP”文本框输入需要的接口IP地址。 **注意**: • 修改任意接口的IP地址后，所有登录中的用户均需要重新登录智源平台。 • 不同接口所属的网段不能重合。
接口掩码	在部署智源平台时，可通过CLI配置接口的子网掩码，此处显示已配置的接口子网掩码。如需修改，在“接口掩码”文本框输入需要的子网掩码。

3. 点击“确定”，完成配置。

网络配置

配置智源平台的网络相关参数，请按照以下步骤进行操作:

1. 点击“系统设置 > 网络管理”，打开<网络管理>页面。下图为集群部署模式下的页面，单机部署时页面中不支持“集群IP”，请根据具体情况进行分析。

2. 点击“编辑”按钮。



在“网络管理”页面，填写网络相关参数。

选项	说明
集群IP	在集群部署环境中，此处显示智源平台集群的虚拟IP地址（VIP）。
网关	指定网关IP地址。
DNS服务器	
首选服务器	指定首选DNS服务器的IP地址。
备用服务器	指定备用DNS服务器的IP地址。

3. 点击“确定”按钮，保存当前页面所做配置。

证据信息管理

针对智源平台检测出的威胁事件，用户可以配置证据信息报文存储功能，将探针收集到的触发威胁事件的原始流量作为对应的证据信息进行保存，以便后续查看、分析证据信息，从而对威胁事件产生原因进行详细分析。

配置证据信息报文存储功能相关参数，请按照以下步骤进行操作：

1. 点击“系统设置>证据信息管理”，打开“证据信息管理”页面。



2. 默认情况下，证据信息报文存储功能为开启状态。如果当前处于关闭状态，点击“存储证据信息报文”处的启用按钮，可开启证据信息报文存储功能。
3. 在“存储位置”处点击单选按钮指定证据信息报文的存储位置，可存储在智源平台中或者探针设备中。默认位置为“探针设备”。
4. 如需关闭证据信息报文存储功能，点击启用按钮后，在提示对话框中再次点击“确定”按钮。

配置完成后，即可在“威胁分析>威胁>事件”页面中，威胁事件详情页<证据信息>中下载证据信息报文。详细操作请参阅查看威胁详细信息。

注意:

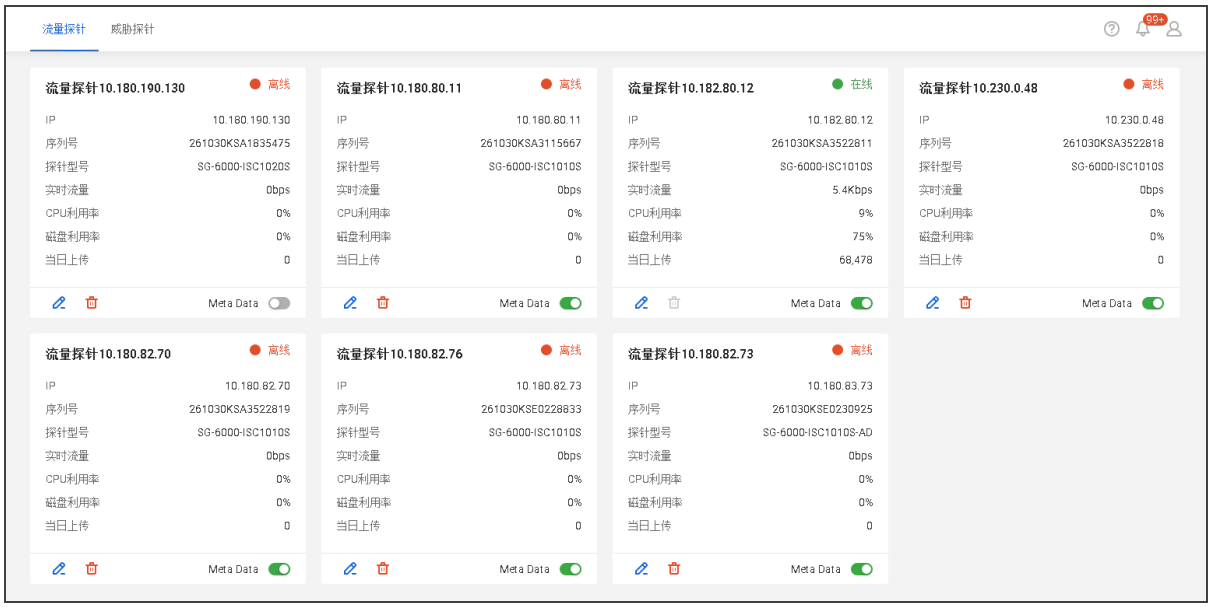
- 如果证据信息报文的存储位置为探针设备，只有当探针设备与智源平台处于已连接状态时，才能对产生的威胁事件下载证据信息。
- 如果修改了证据信息报文的存储位置，则不能下载修改位置前产生的威胁事件对应的证据信息。
- 证据信息报文存储功能关闭后，关闭前产生的威胁事件对应的证据信息可以正常下载，关闭后产生的威胁事件证据信息将不能下载。
- 当探针设备或者智源平台的证据信息报文存储空间的占用率达到最大限制时，最早存储的报文会开始老化，老化后的报文将不能下载；同时，当证据信息报文在探针设备或者智源平台的存储时间超过365天后，也将不能继续下载。

探针管理

探针管理指查看与智源平台管理的探针（流量探针、威胁探针）详细信息，包括探针状态、IP地址、序列号、探针型号、实时流量、当日日志上传数量等。

流量探针

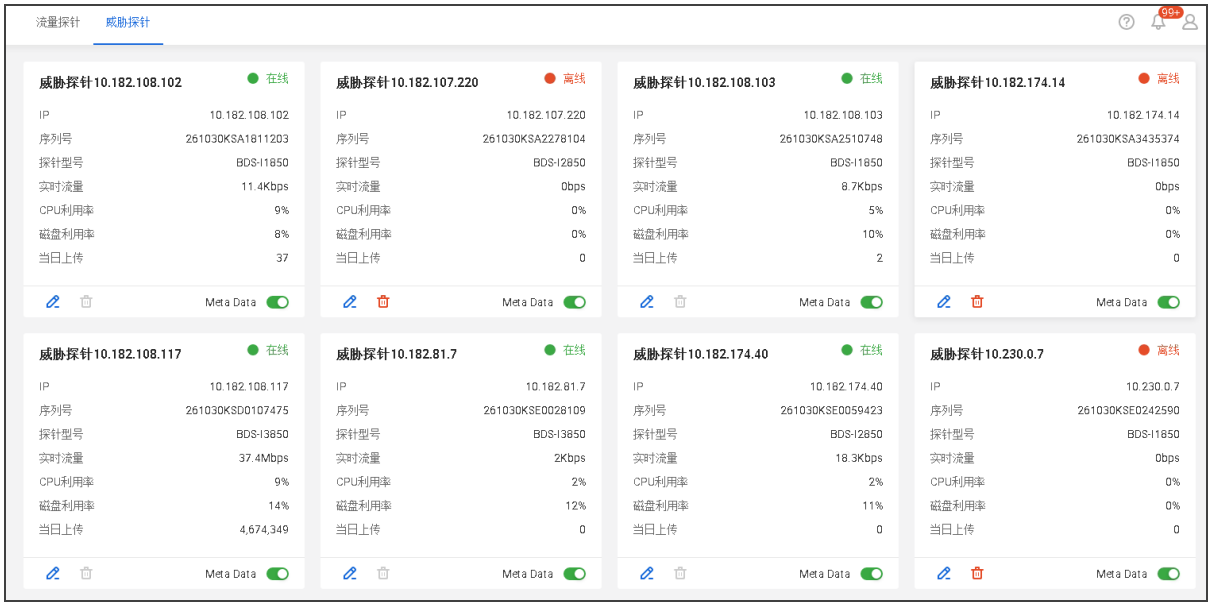
点击“系统设置>探针管理>流量探针”，打开流量探针管理页面。



- 点击流量探针信息中的 按钮，打开“修改名称”页面，编辑所选流量探针的名称。
- 点击流量探针信息中的 按钮，删除所选流量探针。
- 点击“Meta Data”处 按钮，开启或关闭接收所选探针的数据源信息。 表示接收， 表示不接收。

威胁探针

点击“系统设置>探针管理>威胁探针”，打开威胁探针管理页面。



- 点击威胁探针信息中的 按钮，打开“修改名称”页面，编辑所选威胁探针的名称。
- 点击威胁探针信息中的 按钮，删除所选威胁探针。
- 点击“Meta Data”处按钮，开启或关闭接收所选探针的数据源信息。表示接收，表示不接收。

级联管理

设备支持与其他智源平台进行级联，用户可在上级平台的威胁分析、弱点分析、风险管理等页面切换至不同的平台，方便监控多个平台的数据。

级联设置

级联设置页面展示当前智源平台的信息，根据需要可以修改平台的名称、级联密码以及联系人信息。若平台没有配置级联密码，则不能被添加为上级平台。

点击“系统设置 > 级联管理”，并选择<级联设置>标签页。



平台信息	
平台名称	展示当前平台的名称。
平台IP	点击“网络管理”，跳转至"网络管理" 在第492页页面查看和修改当前平台的IP。 • 若当前平台为下级平台，修改平台IP地址后，会断开和上级平台原有的连接，并自动发起新的连接。 • 若当前平台为上级平台，修改平台IP地址后，会断开和所有下级平台的连接。若重新修改回原来的IP地址，那么下级平台将重新自动连接。
端口号	展示当前平台的级联端口号。
级联密码	不支持查看，仅支持编辑，具体配置方法请参阅编辑级联设置部分。
SN号	展示当前平台的SN号。
平台联系人	
姓名	展示联系人的姓名。
手机号码	展示联系人的手机号码。
邮箱账号	展示联系人的邮箱账号。

编辑级联设置

编辑级联设置，请按照以下步骤进行操作：

1. 点击“系统设置 > 级联管理”，并选择<级联设置>标签页。
2. 点击页面下方“编辑”按钮，编辑平台信息以及平台联系人的信息。



编辑级联设置，配置以下参数。

选项	说明
平台名称	指定本平台的名称，可输入值范围为0至64个字符。若未指定平台名称，当本平台与其他平台级联时，“平台名称”处显示平台的IP地址。若本平台已连接上级平台，修改平台名称后，将会同步给上级平台。
级联密码	指定级联密码。其他平台将本平台绑定为上级平台时，须输入本平台的级联密码。（绑定上级平台的配置方法，请参考编辑上级平台信息部分。）密码可由数字和字母组成，长度为6至10位。修改级联密码后，所有已连接的下级平台均会断开；若将级联密码重新修改为原密码，那么下级平台将重新自动连接。
联系人	点击下拉菜单打开联系人列表，选择平台的联系人，仅可单选。若本平台已连接上级平台，修改联系人信息后，将会把新的联系人信息同步给上级平台。 • 在搜索框中输入指定的联系人名称，点击 搜索指定

选项	说明
	的联系人。 • 如果联系人列表中没有需要的联系人，可点击“新建联系人”，在弹出的<新建联系人>页面，新增联系人信息。 • 点击“清空选项”，清空“责任人”选项中已选择的区域责任人。

3. 点击“确定”，保存配置。

下级平台管理

下级平台管理页面展示了与本平台绑定的下级平台的信息，包括平台信息、联系人信息以及连接状态信息。一个平台最多可以绑定30个下级平台。

点击“系统设置 > 级联管理”，并选择<下级平台管理>标签页。



- 点击列表上方 筛选 0 按钮，然后在弹出部分选择筛选条件，系统将根据筛选条件筛选特定的下级平台信息。圆圈中的数字表示已配置筛选条件的个数，点击 “重置”按钮，删除已经添加的筛选条件。
- “连接状态”列展示了本平台与下级平台的连接状态，包括“连接成功”和“连接失败”两种。
- 点击下级平台后的 按钮，删除下级平台。若下级平台的状态为“连接失败”，删除操作仅将该平台的数据从列表中删除，当下级平台恢复连接并自动绑定到上级平台时，上级平台的列表中会

正常显示此下级数据；若下级平台的状态为“连接成功”，删除操作会将该平台数据从列表中删除，同时将清空该下级平台的<上级平台管理>页面的基础配置信息。

上级平台管理

上级平台管理页面展示了本平台与上级平台的连接状态以及上级平台的信息，支持编辑上级平台的信息，同时支持配置上送到上级平台的数据范围。

基础配置

点击“系统设置 > 级联管理”，选择<上级平台管理>标签页，并选择<基础配置>标签页。



- “连接状态”展示本平台与上级平台的连接状态，包括“成功”和“失败”，当状态为“失败”时展示失败的原因。若本平台没有绑定上级平台，“连接状态”显示为“未绑定上级平台”。
- “上级平台信息”部分展示上级平台的名称、IP、端口号、级联密码以及SN号信息。平台名称、IP以及级联密码需要用户手动输入，端口号和SN号在成功绑定上级平台后自动获取。若本平台没有绑定上级平台，则该部分内容为空。
- 点击“编辑”按钮，编辑与本平台绑定的上级平台的信息，具体配置请参考编辑上级平台信息部分。
- 点击“清空连接信息”按钮，将解除本平台与上级平台的连接，清空本平台中上级平台的信息，同时在上级平台中显示该设备连接失败。若本平台没有绑定上级平台，该按钮置灰不可点击。

编辑上级平台信息

在本平台上绑定上级平台或编辑上级平台的信息，请按照以下步骤进行操作：

1. 点击“系统设置 > 级联管理”，选择<上级平台管理>标签页。
2. 选择<基础配置>标签页，点击“编辑”按钮，进入上级平台信息的编辑页面。



编辑上级平台信息，配置以下参数。

选项	说明
平台IP	输入上级平台的IP地址。
端口号	输入上级平台的端口号。
级联密码	输入上级平台的级联密码。

3. （可选）点击“连通测试”按钮，测试本平台是否能够与该平台级联，结果将显示“成功”或“失败”。

4. 点击“确定”，完成配置，本平台会立刻与配置的平台进行连接。

注意: 下级平台完成绑定上级平台后，若出现下级平台或上级平台重启，或者心跳超时的情况，下级平台将进行自动重连。首次重连等待时间为10s，若重连失败，此后重连等待时间每次增加10s，最长为120s。在上级平台信息的编辑页面，点击“确定”后将重置重连等待时间。

上报数据配置

点击“系统设置 > 级联管理”，选择<上级平台管理>标签页，并选择<上报数据配置>标签页。

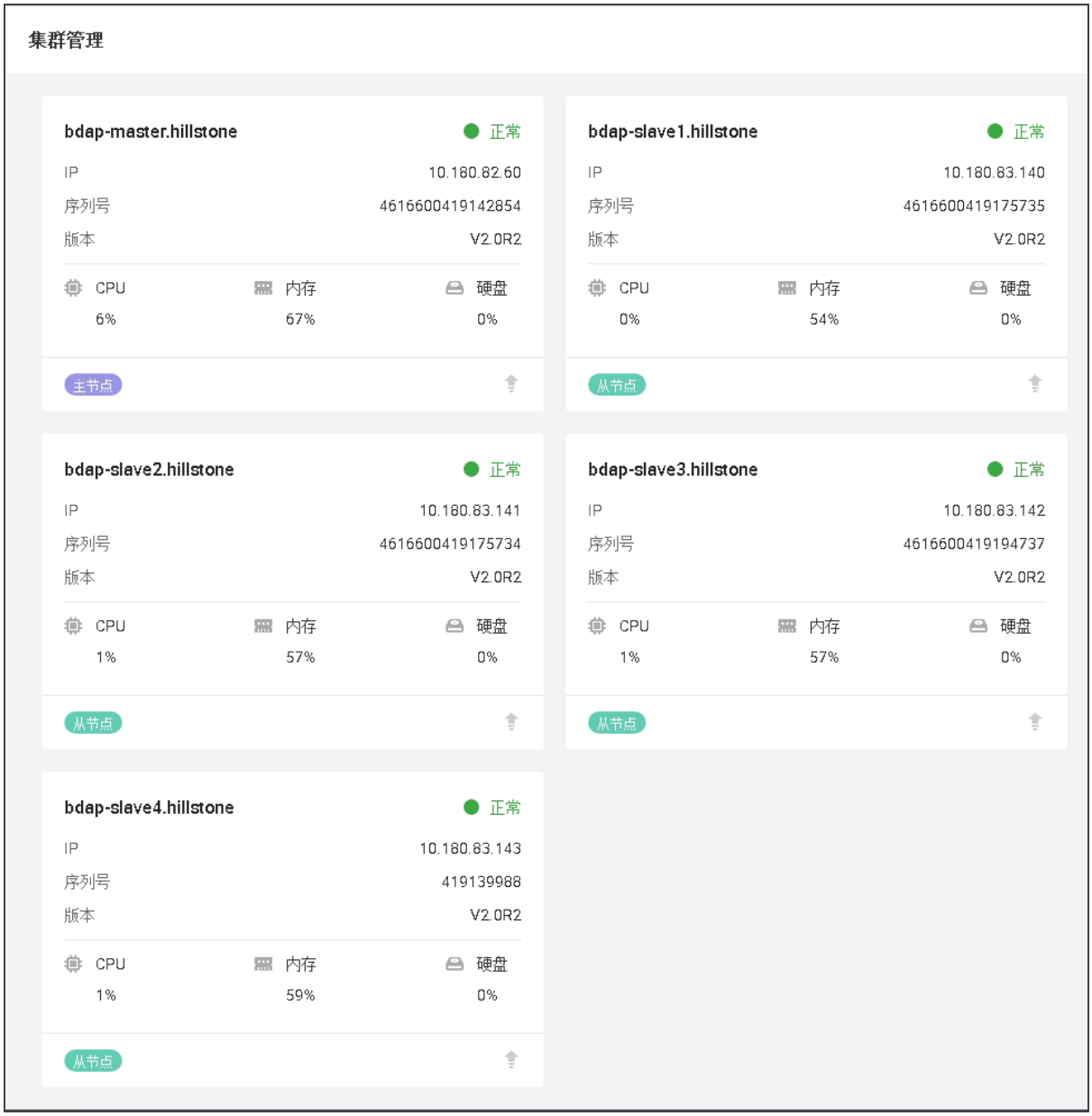


- 点击“数据上报”后的启用按钮，本平台将符合指定范围内的数据上送给上级平台。若禁用数据上报，则本平台不会将数据上送到上级平台。默认情况下为启用状态。
- 勾选“事件状态”和“事件级别”后的复选框，选择上送数据的范围，默认全选。
- 点击“恢复默认”按钮，将页面上的配置恢复成默认状态。
- 点击“保存”按钮，保存页面上的修改。

集群管理

集群管理指查看智源平台集群中的所有设备的详细信息，包括IP地址、序列号、系统版本以及硬件相关信息（CPU、内存、磁盘）。当使用单台部署的时候，在<集群管理>页面中以主节点来显示该设备的详细信息。

点击“系统设置>集群管理”，打开“集群管理”页面。



- 当从节点（Slaver）的系统版本低于主节点（Master）时，设备将会自动升级从节点的系统版本，使得版本保持一致。
- 若系统版本未自动升级，用户还可以在从节点信息处，点击右下角按钮进行手动升级从节点的系统版本。
- 当右下角显示为按钮时，表示已经自动升级完成，无需进行手动升级。

安全分析计划

安全分析计划是一项将智源平台的威胁事件上报山石云·景，便于安全分析人员对威胁事件进行分析，从而提高检测的准确性、提升用户体验的计划。

山石云·景是一款安全领域的SaaS产品，更多信息请参阅《山石云·景常见问题手册》。



注意: 目前，该计划仅支持将智源平台的威胁事件上报山石云·景供安全分析人员进行分析，暂不支持山石云·景其他功能。

开启加入山石安全分析体验计划后：

- 智源平台每隔十分钟将所有类型的威胁事件上报至山石云·景。
- 智源平台每次上报的威胁事件数目上限为1000条。
- 山石云·景接收威胁事件的默认服务器配置如下，且不可变更：
  - 地址：cloudview.hillstonenet.com.cn；用户名：defaultAccount；密码：空。

启用/禁用安全分析计划

启用/禁用安全分析计划，请按照以下步骤进行操作：

1. 选择“系统设置>安全分析计划”，打开安全分析计划页面。
2. 点击启用/禁用按钮，选择启用/禁用山石安全分析体验计划。默认为禁用状态。

人行数据对接

智源支持与人民银行金融行业态势感知与信息共享平台进行数据对接，可将智源平台中指定数据上报至对接的人民银行金融行业态势感知与信息共享平台，并且支持在智源平台中查看上报的历史数据信息以及上报状态。

数据对接配置

与人行数据对接的配置包括以下内容：

- 开启/关闭人行数据对接功能
- 基础配置：配置对接机构信息、防病毒设备数量及指定数据上报途径
- 上报数据配置：配置上报的数据内容类型以及指定数据的筛选条件

开启/关闭人行数据对接功能

开启或关闭人行数据对接功能，请按照以下步骤进行操作：

1. 选择“系统设置 > 人行数据对接”，进入人行数据对接页面。
2. 在<数据对接配置>标签页，点击“数据上报”的“启用”按钮，开启或关闭人行数据对接功能，并在下方表单中配置正确的数据，以确保数据正常上报。



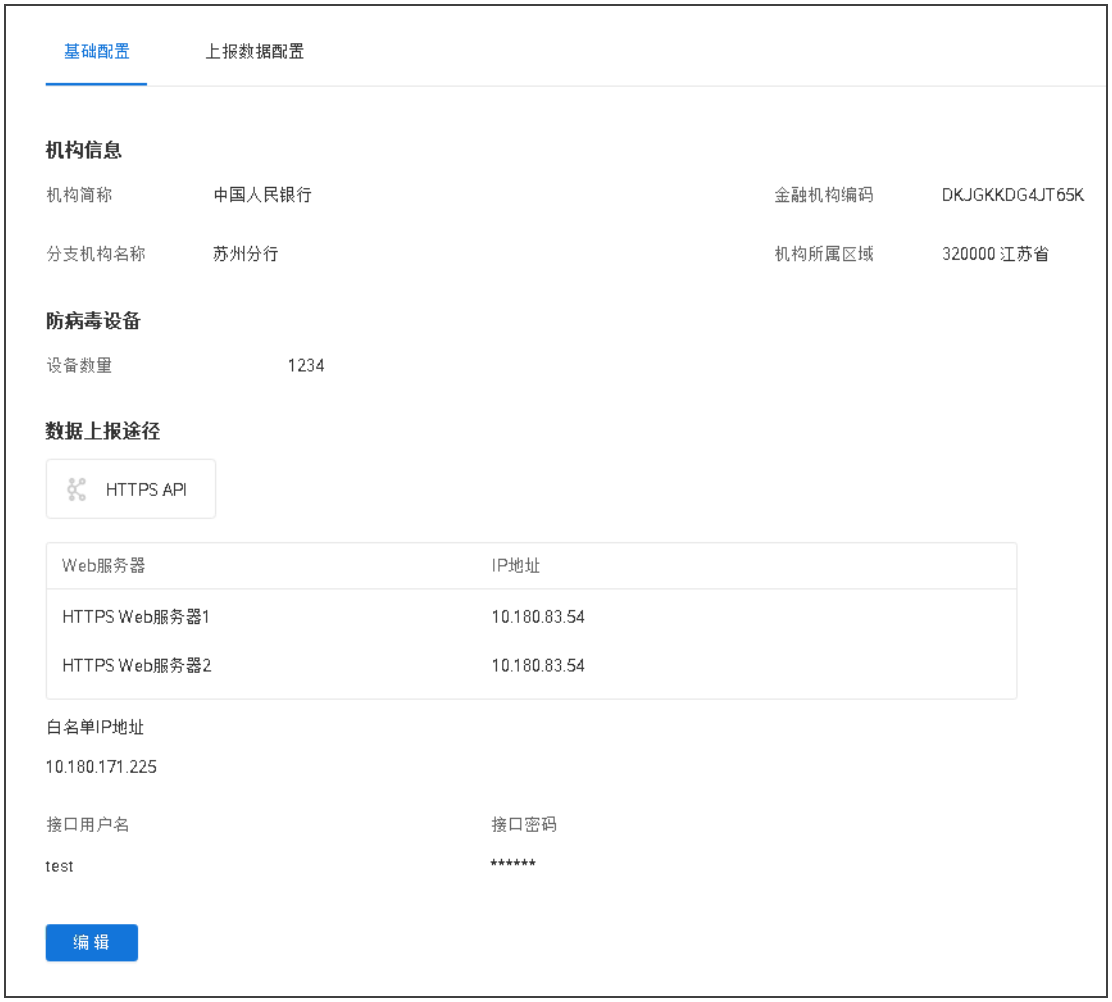
基础配置

用户可配置机构信息、防病毒设备数量及指定数据上报途径。

配置数据对接功能的基本配置信息，请按照以下步骤进行操作：

1. 选择“系统设置 > 人行数据对接”，进入人行数据对接页面。

2. 在<数据对接配置>标签页，选择<基础配置>标签页。



3. 点击页面下方的“编辑”按钮，对人行数据对接功能进行基本配置。

选项	说明
机构信息	
机构简称（必填项）	输入机构简称。例如：“中国人民银行”。
金融机构编码（必填项）	输入分支机构从中国人民银行申领的指代其身份的特定代码，需符合金融机构编码规范（JR/T0124-2014）标准要求。例如：“DKJGKKDG4JT65K”。

选项	说明
分支机构名称（必填项）	输入分支机构名称。例如“苏州分行”。
机构所属区域（必填项）	从下拉列表中选择机构所属区域。选择后，将会自动显示对应区域的行政区划代码。例如：“320000 江苏省”。
防病毒设备	
设备数量（必填项）	输入分支机构部署的防病毒设备的数量。

数据上报途径（必填项）	指定数据上报的途径，选项包括KAFKA和HTTPS API。
	• KAFKA：使用KAFKA数据总线接入方式上报数据。
	  • 映射IP地址（必填项）：分别输入3个KAFKA服务器psoc.kafka.node1、psoc.kafka.node2和psoc.kafka.node3的映射IP地址。输入映射IP地址后，才可连接到KAFKA服务器，从而通过KAFKA服务器正常发送数据和获取数据。3个映射IP地址须同时指定。
	• HTTPS API：使用HTTPS API接口方式上报数据。
	  • IP地址（必填项）：分别输入HTTPS Web服务器1和HTTPS Web服务器2的IP地址。2个IP地址须同时指定。
	  • 白名单IP地址（必填项）：输入白名单IP地址。在使用HTTPS API接口前，分支机构须先配置并报备本机构IP白名单信息，由中国人民银行总行同意开通权限后，方可使用该HTTPS API接口。
	  • 接口用户名（必填项）：输入人民银行金融行业态势感知与信息共享平台提供给分支机构的接口用户名（非HTTPS应用登录名）。
	  • 接口密码（非必填项）：输入以上接口用户名的接

选项	说明
	口密码。

上报数据配置

用户可以指定上报的日志数据的内容类型及过滤条件，将过滤后的日志数据上报至对接的人民银行金融行业态势感知与信息共享平台。

1. 选择“系统设置 > 人行数据对接”，进入人行数据对接页面。
2. 在<数据对接配置>标签页，选择<上报数据配置>标签页。



3. 点击页面底部的“编辑”按钮，配置上报的日志数据的内容类型及过滤条件。

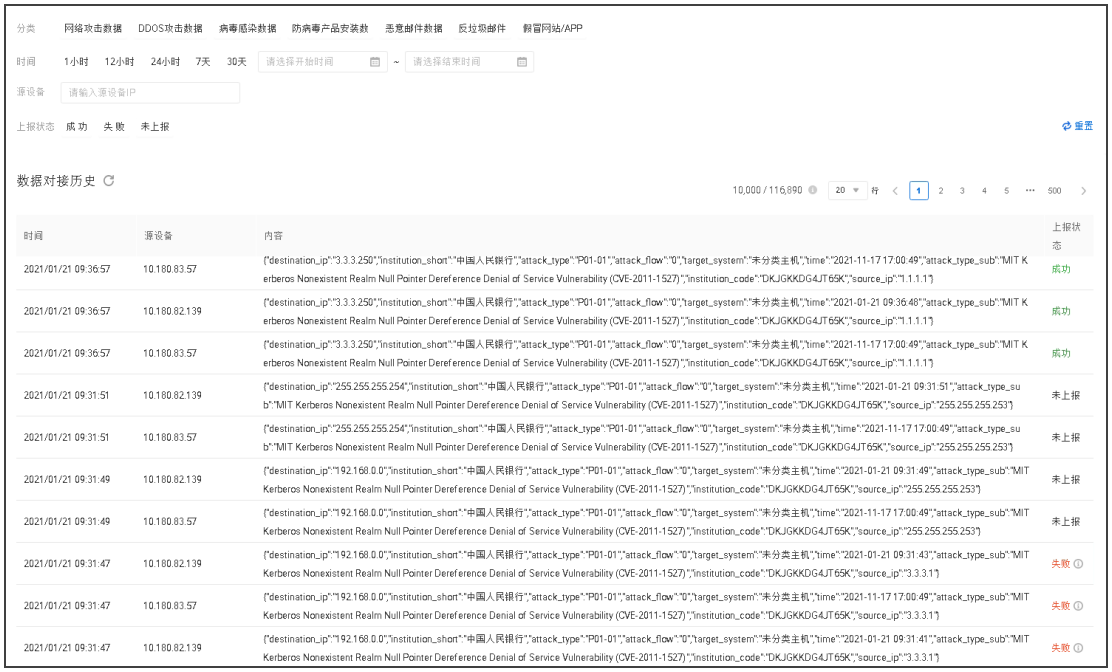
选项	说明
上报数据内容	点击复选框，选择上报日志的数据类型。选项包括“网络攻击数据”、“DDOS攻击数据”、“病毒感染数据”、“防病毒产品安装数”、“恶意邮件数据”、“反垃圾邮件”和“假冒网站/APP”，可多选。
上报数据过滤	
日志源IP	指定上报日志的源IP地址。指定后，智源仅上报指定源IP地址的日志数据。 可输入IP地址或IP地址范围，然后点击“添加”按钮，即可添加上报日志的源IP地址或源IP地址范围。 若输入单个IP地址，可在“起始IP地址”或“结束IP地址”任一文本框中填写。
日志源端口	指定上报日志的源端口号。指定后，智源仅上报指定源端口的日志数据。 可输入端口号或端口号范围，然后点击“添加”按钮，即可添加上报日志的源端口号或源端口号范围。 若输入单个端口号，可在“起始端口”或“结束端口”任一文本框中填写。
日志目的IP	指定上报日志的目的IP地址。指定后，智源仅上报指定目的IP地址的日志数据。 可输入IP地址或IP地址范围，然后点击“添加”按钮，即可添加上报日志的目的IP地址或目的IP地址范围。 若输入单个IP地址，可在“起始IP地址”或“结束IP地址”任一文本框中填写。
日志目的端口	指定上报日志的目的端口号。指定后，智源仅上报指定目的端口的日志数据。 可输入端口号或端口号范围，然后点击“添加”按钮，即可添加上报日志的目的端口号或目的端口号范围。 若输入单个端口号，可在“起始端口”或“结束端口”任一文本框中填写。

选项	说明
安全设备主机IP	指定上报日志的来源安全设备主机IP。智源从不同的安全设备主机收集日志数据，在用户指定特定的安全设备主机IP后，智源仅上报来自该安全设备主机的日志数据。 可输入IP地址或IP地址范围，然后点击“添加”按钮，即可添加安全设备主机的IP地址或IP地址范围。 若输入单个IP地址，可在“起始IP地址”或“结束IP地址”任一文本框中填写。

4. 点击“确认”按钮，保存当前页面所作配置。

数据对接历史

<数据对接历史>页面展示上报到人民银行金融行业态势感知与信息共享平台的历史数据信息以及上报状态。



- 在页面上方，用户可指定以下条件对历史数据进行过滤，被筛选出的数据信息将显示在下方的数据对接历史列表中。点击“ 重置 ”按钮，恢复默认的筛选条件。

- 分类：指定数据信息的分类，选项包括“网络攻击数据”、“DDOS攻击数据”、“病毒感染数据”、“防病毒产品安装数”、“恶意邮件数据”、“反垃圾邮件”和“假冒网站/APP”。可多选。
- 时间：指定数据上报的时间范围，选项包括“1小时”、“12小时”、“24小时”、“7天”、“30天”及自定义时间范围。仅可单选。
- 源设备：指定数据的来源安全设备主机IP。
- 上报状态：指定数据的上报状态，选项包括“成功”、“失败”及“未上报”。可多选。

- 在页面下方的数据对接历史列表中，用户可查看历史数据的上报时间、源设备IP、内容及上报状态。
  - 若某数据条目的上报状态显示“失败”，将鼠标悬浮在“失败”旁边的图标之上，该数据条目的上报失败原因即可自动显示。
  - 点击“数据对接历史”旁的 按钮，即可刷新数据对接历史列表，查看最新的上报数据信息。

智源支持与人民银行金融行业态势感知与信息共享平台进行数据对接，可将智源平台中指定数据上报至对接的人民银行金融行业态势感知与信息共享平台，并且支持在智源平台中查看上报的历史数据信息以及上报状态，实现金融行业安全数据的集中和共享，使得人民银行总部能够全面掌握金融行业内的安全数据。

恢复出厂设置/退出/重启/关机

恢复出厂设置

目前，智源平台仅支持通过reset命令行方式恢复设备的出厂设置，执行后，需要进一步选择以下选项：

- a：清除所有配置信息、存储的数据，保留已安装的许可证。
- b：清除所有配置信息、存储的数据以及安装的所有许可证。
- c：取消该恢复出厂设置操作。

退出登录

退出当前登录的用户账户，请按照以下步骤进行操作：

1. 点击系统页面右上角  按钮。
2. 在弹出框中点击“退出登录”按钮。
3. 退出登录后，将会返回系统登录页面。

重启系统

重启智源平台系统，请按照以下步骤进行操作：

1. 点击系统页面右上角  按钮。
2. 在弹出框中点击“重启”按钮。
3. 在<提示>页面中，点击“确定”按钮后，系统将会开始重启。

关机

关闭智源平台系统，请按照以下步骤进行操作：

1. 点击系统页面右上角  按钮。
2. 在弹出框中点击“关机”按钮。
3. 在<提示>页面中，点击“确定”按钮后，系统将会关闭。