**数据泄露网络防护系统**

**用户手册  
版本号：【V1.5】**



杭州世平信息科技有限公司

版权声明

本手册中的所有内容及格式的版权属于杭州世平信息科技有限公司（以下简称世平信息）所有，未经世平信息许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有 不得翻印 © 2016 杭州世平信息科技有限公司

商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

SHIPING INFO ® 杭州世平信息科技有限公司

信息反馈

<http://www.shipinginfo.com>

目 录

[欢迎使用本指南 6](#_Toc454372699)

[读者对象 6](#_Toc454372700)

[1 系统概述 7](#_Toc454372701)

[1.1 系统简介 7](#_Toc454372702)

[1.2 策略概述 8](#_Toc454372703)

[1.3 策略所包含的内容 8](#_Toc454372704)

[1.3.1 关联目标 8](#_Toc454372705)

[1.3.2 发现扫描规则 8](#_Toc454372706)

[1.3.3 规则组 8](#_Toc454372707)

[1.3.4 数据资源和高级资源 8](#_Toc454372708)

[1.3.5 预定义资源、规则和规则组 9](#_Toc454372709)

[2 快速入门 9](#_Toc454372710)

[2.1 登录系统 10](#_Toc454372711)

[2.2 系统布局 11](#_Toc454372712)

[2.3 系统菜单 11](#_Toc454372713)

[2.3.1 路径导航 11](#_Toc454372714)

[2.3.2 向导 12](#_Toc454372715)

[2.3.3 注销 12](#_Toc454372716)

[2.3.4 帮助 12](#_Toc454372717)

[2.3.5 关于 12](#_Toc454372718)

[2.3.6 更改用户密码 12](#_Toc454372719)

[2.3.7 系统页码导航 13](#_Toc454372720)

[2.4 快速配置 13](#_Toc454372721)

[3 系统功能 14](#_Toc454372722)

[3.1 系统管理员 14](#_Toc454372723)

[3.1.1 查看系统状态 15](#_Toc454372724)

[3.1.2 组织资源管理 16](#_Toc454372725)

[3.1.3 个人中心 17](#_Toc454372726)

[3.1.4 角色管理 18](#_Toc454372727)

[3.1.5 用户管理 20](#_Toc454372728)

[3.1.6 认证设置 22](#_Toc454372729)

[3.1.7 告警管理 23](#_Toc454372730)

[3.1.8 告警阈值设置（系统告警阈值设置） 26](#_Toc454372731)

[3.1.9 数据备份/恢复 26](#_Toc454372732)

[3.1.10 日志服务器设置 27](#_Toc454372733)

[3.1.11 许可管理 28](#_Toc454372734)

[3.1.12 基本设置 28](#_Toc454372735)

[3.1.13 升级管理 29](#_Toc454372736)

[3.1.14 信任主机管理 30](#_Toc454372737)

[3.1.15 网络管理 31](#_Toc454372738)

[3.2 安全管理员 37](#_Toc454372739)

[3.2.1 查看系统状态 39](#_Toc454372740)

[3.2.2 业务资源管理 39](#_Toc454372741)

[3.2.3 地理映射 40](#_Toc454372742)

[3.2.4 主机资源管理 42](#_Toc454372743)

[3.2.5 网络资源管理 46](#_Toc454372744)

[3.2.6 数据资源管理 48](#_Toc454372745)

[3.2.7 高级资源管理 57](#_Toc454372746)

[3.2.8 发现扫描规则管理 65](#_Toc454372747)

[3.2.9 网络防护规则管理 69](#_Toc454372748)

[3.2.10 网络防护策略管理 75](#_Toc454372749)

[3.2.11 网络防护事件管理 80](#_Toc454372750)

[3.2.12 全局状态设置 85](#_Toc454372751)

[3.2.13 报表计划任务 85](#_Toc454372752)

[3.2.14 全球数据态势感知 89](#_Toc454372753)

[3.2.15 报表风格设置 90](#_Toc454372754)

[3.2.16 网络防护报表 90](#_Toc454372755)

[3.2.17 任务中心 95](#_Toc454372756)

[3.2.18 个人中心 99](#_Toc454372757)

[3.2.19 角色管理 100](#_Toc454372758)

[3.2.20 用户管理 102](#_Toc454372759)

[3.2.21 安全日志维护 104](#_Toc454372760)

[3.2.22 信任主机管理 106](#_Toc454372761)

[3.2.23 密码安全策略设置 107](#_Toc454372762)

[3.3 安全审核员 107](#_Toc454372763)

[3.3.1 个人中心 108](#_Toc454372764)

[3.3.2 角色管理 109](#_Toc454372765)

[3.3.3 用户管理 111](#_Toc454372766)

[3.3.4 日志维护 113](#_Toc454372767)

[3.3.5 系统操作日志 115](#_Toc454372768)

[3.3.6 告警管理 115](#_Toc454372769)

[3.3.7 信任主机管理 115](#_Toc454372770)

# 欢迎使用本指南

欢迎使用杭州世平信息科技有限公司（以下简称“世平信息”）数据卫士-敏感信息管理系统-数据泄露网络防护系统（以下简称“SIMP-DPS”）系列产品。

本指南描述如何使用SIMP-DPS，提供概念性和描述性信息，包括使用流程、功能说明、以及管理配置等信息。

# 读者对象

本指南的读者对象为使用本系统的系统管理员、安全管理员、安全审核员用户。通过阅读本文档，可以完成以下一些工作：

* SIMP-DPS基本设置
* SIMP-DPS权限管理
* 制定网络防护策略
* 报表管理
* 管理与配置SIMP-DPS的附加功能模块，如数据备份/恢复、日志维护等。

# 系统概述

## 系统简介

数据卫士-敏感信息管理系统，英文型号：SIMP。SIMP包含以下子系统：

数据泄露网络防护系统（Data leakage network Prevention System，英文子型号：DPS；以独立产品出现，简称为“SIMP-DPS”）为世平信息SIMP产品体系中的基础系统，核心功能是对网络传输中的数据进行深度内容分析，集成多种内容检测技术，对传输过程中的数据进行实时监控及防护；一旦存在敏感数据违规传输，系统将对其实时阻止或隔离，主动防止敏感数据丢失；同时为确保设备的可实施性，提供灵活的策略框架，系统提供简化的策略配置过程。

SIMP-DPS的功能如下：

* 监控敏感数据的网络传输，对数据内容进行检测；
* 发现违规传输的敏感数据，系统将对其实现实时的阻止或隔离；
* 基于内容识别的检测技术，识别的精确度高。系统采用的检测技术如下：
  + - 关键字：中文简体、中文繁体、英文、数字；
    - 关键字组：关键字及其权重的集合；
    - 匹配模式：正则表达式、逻辑关系匹配脚本；
    - 文档特征：文档类型；
    - 文档指纹：精确文档指纹（全文档指纹）、模糊文档指纹（文档段或关键语句）；
    - 数据库指纹：精确数据库指纹（每条记录的若干字段组合）；
    - 二维智能学习：二分类匹配特征提取（正例、反例样本特征自学习）；
* 系统提供对策略增加、修改、删除等应用功能。
* 基于角色的事件及报表审计：根据不同角色权限，实现 “网络防护事件”的查询、统计与报表显示。

## 策略概述

网络防护策略是通过配置规则条件实现对违规传输的敏感数据进行防护的目的。创建网络防护策略时，可以根据HTTP(S)、FTP、SMTP协议类型来创建。

## 策略所包含的内容

### 关联目标

关联目标是策略需要监控及保护的数据源IP地址及目的IP地址，系统默认源IP地址和目的IP地址为“任意地址”。

### 发现扫描规则

发现扫描规则由各类数据资源的逻辑关系组合构成，是数据监控及防护的核心条件，每个规则可设置相应的敏感度。

### 规则组

规则组由多个规则组成，规则组包括发现扫描规则组。

发现扫描规则组由发现规则组成，其中每个规则具有各自的敏感度。每个发现扫描规则组必须关联企业的实际业务资源（详见下文描述），该业务资源在“管理资源”中定义。

### 数据资源和高级资源

数据资源包括文档特征、关键字（组）、匹配模式等，作为基本的内容检测技术。

* 文档特征包括文档的类型、文档体积以及文档名称。
* 关键字（组）定义一个或多个关键字，用于待检测数据的匹配。
* 匹配模式定义一个正则表达式，同时可以定义一个排除的正则表达式或多个关键字，以便更精确的描述检测条件。
* 高级资源包括文档指纹、数据库指纹、二维智能学习。
* 文档指纹包括精确文档指纹和相似度文档指纹，精确指纹采用快速散列算法对整个文件进行处理，生成其特征，并存储到指纹数据库。相似度指纹通过自然语言处理技术，并结合相应的指纹算法，提取其特征，并存入指纹数据库，可以支持部分匹配检测。
* 数据库指纹将数据库中每条记录的指定字段通过指纹算法处理后录入指纹数据库，系统利用该指纹可以检测待处理数据中是否存在数据库中的记录信息。
* 二维智能学习通过处理少量敏感数据样本和非敏感数据样本，生成模型，系统可以基于该模型对其他数据进行检测，找出其中的敏感数据。

### 预定义资源、规则和规则组

在总结各行业数据泄漏防护需求的基础上，系统预置了多种数据资源、规则和规则组。预定义数据资源包括关键字（组）、匹配模式、各种匹配脚本（如：身份证识别、银行卡识别、电话识别、各类源码识别、行业报表、行业术语字典等）。预定义规则由上述数据资源的不同逻辑组合构成。根据不同的行业，结合国家、行业的法律和合规要求，系统将同类规则形成预定义规则组。

# 快速入门

本章介绍如何正确登录系统以实现管理与配置。

本章描述：

* 登录系统
* 系统布局
* 快速配置

## 登录系统

通过Web浏览器登录系统，实现基于WEB的管理。

三权用户及登录初始密码如下：

|  |  |  |
| --- | --- | --- |
| 用户所属角色 | 用户名 | 密码 |
| 系统管理员 | sysadmin | Spinfo0123 |
| 安全管理员 | secadmin | Spinfo0123 |
| 安全审核员 | adtadmin | Spinfo0123 |

具体操作流程：

1. 配置直连主机ip地址为192.168.1.101，打开Web 浏览器（建议使用ChromeV45+浏览器），地址栏键入系统管理地址“https://系统ip地址”（缺省管理端口为ETH0，地址为：https://192.168.1.100。
2. 进入系统的登录页面:



1. 在“用户名”框中，键入用户名(首次登录请使用系统管理员帐户登录，缺省用户名为：sysadmin)。
2. 在“密码”框中，键入系统管理员分配的密码（缺省密码为：Spinfo0123）。
3. 点击【登录】按钮。系统将打开状态模块全局概览视图。

|  |
| --- |
| 注意：  用户首次登录时不需要输入【验证码】，如果密码输入错误下次登陆时则需要输入验证码重新登录系统；  首次登录请设置系统邮件服务器，将用户单位可用邮件服务器信息进行设置，并将管理员邮箱设置为邮件服务器可达的邮件地址，以确保忘记密码时进行恢复操作；  如果忘记密码无法登录系统时，请使用系统提供的忘记密码功能，输入帐号名称和注册用户时提供的认证邮箱地址即可找回密码。 |

## 系统布局

本节为您介绍如何操作系统界面。本节描述：

* 系统菜单
* 路径导航
* 【向导】
* 【注销】
* 【帮助】
* 关于
* 更改“用户密码”
* 系统页码导航

## 系统菜单

在系统中，左侧窗格称为管理菜单，包含允许用户在系统模块之间切换的按钮。系统右侧窗格称为内容窗格，显示内容根据左侧所选择的管理菜单。

### **路径导航**

在系统中，路径导航显示在内容窗格顶部，指示用户当前访问页面的全部路径。路径为超链接形式，点击超链接可转至相关页面。

### **向导**

在系统中，【向导】按钮显示在功能菜单的右上角，仅三权分立用户具有使用向导功能权限。其他用户不具备使用向导功能权限。

三权分立用户首次登录系统时，系统将显示不同的向导页面。

三权分立用户指：系统管理员（sysadmin）、安全管理员（secadmin）、安全审核员（adtadmin）。

### **注销**

要退出并返回到系统登录窗口，请点击位于窗口右上方的【注销】按钮。

### **帮助**

提供系统帮助信息。

### **关于**

显示当前系统名称、版本号等信息。

### **更改用户密码**

点击窗口右上方登录的【用户名】超链接，或点击“系统”>“个人中心”菜单，可以查看当前登录用户的详细信息，并能够修改当前用户的密码。操作步骤如下：

1. “当前密码”字段中输入当前有效的密码。
2. 在“新密码”和“确认密码”字段中输入您的新密码。
3. 点击【确定】按钮保存，下次登录时使用新密码。

### **系统页码导航**

在系统内容窗格的数据列表中，当显示数据超出一页时，您可以使用【页码导航】按钮切换页面，方便您查看数据。

## 快速配置

为保证系统能够正常使用，系统管理员（用户名：sysadmin，初始密码：Spinfo0123）必须完成以下工作：

1. 设置系统的管理端IP地址和扫描IP地址，部署后通过该地址管理本系统和执行扫描策略。

登录系统，选择“系统”>“系统设置”>“网络管理”菜单，在“系统”>“网络管理”页面，选择“网络接口”选项卡选择管理口接口，默认为eth0，点击【修改】按钮，修改系统IP地址，并按指定要求输入其他信息，点击【确定】按钮保存。

此外，还需要根据实际的网络环境设置“工作模式”。

例如，设置“旁路模式”，则需设置业务口（默认为eth1）的IP地址；如果“工作模式”设置为“网桥模式”，则需要设置网桥（br0）或其子接口的IP地址，并且将数据通过的网络接口加入网桥中，若存在VLANID情况时，则同时要设置VLANID；如设置为路由模式，则需要在路由配置中进行具体的路由转换设置。

1. 设置邮件服务器。使用系统邮件告警、报表计划任务、事件上报等功能模块需要发送邮件。如果不设置邮件服务器地址，则无法正常发送邮件。

选择“系统”>“系统设置”>“基本设置”菜单，在“系统”>“基本设置”页面，选择“邮件服务器”选项卡，按指定要求输入SMTP服务器地址、默认发件人地址、及对应的密码信息，点击【确定】按钮保存。

1. 修改系统默认用户的邮箱地址，将邮箱设置为邮件服务器可达的邮件地址。如果不修改默认用户的邮箱地址，则不能正常收取邮件。

系统默认用户指系统管理员（sysadmin）、安全管理员（secadmin）、安全审核员（adtadmin）。

选择“系统”> “用户管理”菜单，分别修改系统默认用户信息，将邮箱地址输入正确，点击【确定】按钮保存。

# 系统功能

系统提供基于三权分立角色的访问控制权限。目前系统提供下列几种管理者角色：

* 系统管理员
* 安全管理员
* 安全审核员

下面将分别介绍上述三种角色所对应的权限功能。

## 系统管理员

在初次使用系统时，需要对系统进行初始配置(详见“快速配置”使用说明)。

作为系统管理员，具备以下权限：

* 状态查看：查看系统运行状态。
* 资源管理：“组织资源”管理。
* 系统设置：“许可管理”、“基本设置”、“日志服务器设置”、“升级管理”、“信任主机管理”。
* 权限管理：“个人中心”、“用户管理”、“角色管理”、“认证设置”。
* 告警管理：“告警管理”、“告警阈值设置”。
* 数据管理：“数据备份/恢复”。

以下将对上述功能分别进行描述。

### 查看系统状态

系统管理员（sysadmin）登录系统后，选择“状态”菜单，显示状态视图，分别显示有“系统信息”、“系统状态”、“系统告警列表”、“告警级别趋势图”。

系统信息：显示当前系统的详细信息。如产品型号、序列号、系统持续运行时间、系统日期、软件版本。

系统状态：实时监控系统当前的运行状态，包括CPU利用率、内存利用率、存储利用率。系统状态每5秒刷新一次。

告警列表：显示触发系统告警的最新15条记录。告警列表显示告警名称、时间、级别、操作信息。系统默认按时间降序排序，如需更改排序方式，可点击需要排序列的表头进行升序或降序排列。如需查看某条告警信息的详细内容，点击该信息的“更多”即可。

告警级别趋势图：统计图分两部分显示，左侧以“环形图”形式统计最近24小时的系统告警信息，右侧以“折线图”形式显示各时间周期内系统告警信息。

* 环形图：环形图以系统的告警事件类别为统计依据，显示各类别告警事件占总告警事件的比重。外部以告警事件级别为统计依据，显示各级别告警事件占总告警事件的比重。
* 折线图：折线图以告警级别为统计依据，默认以“最近24小时”的维度显示告警信息，如需更改时间粒度，可更改折线图右上方的下拉列表内容。系统提供三种时间统计粒度：最近24小时、最近一周、最近一月。

|  |
| --- |
| 提示：   * “状态”页面仅显示当前用户创建并且在【首页报表设定】中显示的报表。 * “状态”页面仅显示柱图、饼图形式的事件报表，暂时不支持表格形式的事件。 * 点击图标可刷新图形内容。 * 安全管理员（secadmin）具有“全局状态设置”模块权限，系统管理员（sysadmin）、安全审核员（adtadmin）无“全局状态设置”模块权限。 |

### 组织资源管理

“组织资源”是企业组织架构下的子单位，可以理解为“部门”。“组织资源”可以关联“业务资源”，也可以关联“系统用户”。

|  |
| --- |
| 提示：   * 组织资源中存在“系统用户”时，不允许删除组织资源。 |

#### 新建组织资源

操作步骤如下：

1. 选择“资源”>“组织资源”菜单，点击【组织添加】选项卡。
2. 在“组织资源”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 组织名称 | 该组织的名称 |
| 上级组织 | 选择该组织所属的“上级组织”，系统默认显示“组织资源” |

#### 编辑组织资源

操作步骤如下：

1. 选择“资源”>“组织资源”菜单，在“组织列表”选项卡中，选择待编辑的组织资源。
2. 在该记录的最右侧点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除组织资源

操作步骤如下：

1. 选择“资源”>“组织资源”菜单，在“组织列表”选项卡中，选择待删除的组织资源记录。
2. 点击该记录右侧的【删除】按钮，在提示窗口，点击【确定】保存。

#### 组织资源模糊查询

系统提供按“组织名称”模糊查询功能。

操作步骤如下：

1. 选择“资源”>“组织资源”菜单，在“组织列表”选项卡中，查询条件中输入“组织名称”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 个人中心

#### 查看用户信息

选择“系统”>“个人中心”菜单，显示当前登录用户的详细信息，包括用户名、电子邮箱地址、当前用户的所属角色。

#### 向导设置

* 自动显示向导：指用户首次登录系统时，系统自动弹出“向导帮助”页面，引导用户使用系统。
* 手动显示向导：指用户首次登录系统时，系统不弹出“向导帮助”页面，如需要使用向导功能，需点击系统页面右上角的【向导】按钮，来进入“向导帮助”页面。

#### 更改密码

修改当前登录用户的密码。操作步骤如下：

1. 点击“系统”>“个人中心”菜单，将打开“个人中心”页面。
2. 在“密码管理”部分，“当前密码”字段中输入当前有效密码。
3. 在“新密码”和“确认密码”字段中输入新密码。
4. 点击【确定】按钮保存，下次登录时使用新密码。

|  |
| --- |
| 注意：  修改当前用户密码时，“当前密码”必须输入正确，否则无法更改密码。另外，“新密码”和“确认密码”输入必须一致，且符合密码复杂度要求，否则无法更改密码。 |

### 用户管理

系统用户即系统管理用户。

#### 新建本地用户

新建本地用户操作步骤如下：

1. 选择“系统”>“用户管理”菜单，点击【新建】按钮。系统将显示“本地用户”页面。
2. 在 “本地用户”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 用户类型 | 系统缺省显示为“本地用户”。 |
| 用户名 | 系统登录账号，登陆帐号必须为“3-12位数字、字母、下划线”组成的字符，区分大小写，不能包含反斜杠(\)，且不允许重名。 |
| 姓名 | 与用户名对应的员工姓名。 |
| 密码 | 与用户名对应的登陆密码。 |
| 确认密码 | 再一次确认密码 |
| 邮箱 | 新建用户的电子邮件地址。该地址必须真实有效，当新建用户成功后，系统将发送邮件到该邮箱地址，邮件内容描述该用户的密码认证认证信息。邮箱地址不允许重复。 |
| 密码发送 | 是否使用邮箱发送注册密码。 |
| 部门 | 当前新建用户所属的“组织资源”。 |
| 角色 | 管理员所属的角色类型，包括：系统管理员、安全管理员、安全审核员。 |
| 失效时间 | 定义该用户失去在其权限范围内操作系统的时间。 |
| 备注 | 备注描述信息 |
| 信任主机 | 添加信任主机，该用户只能在信任主机（IP）下正常访问系统 |

#### 编辑用户

用于修改用户信息。操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择待编辑的用户，点击【修改】按钮。
2. 在“本地用户”页面，按指定要求输入信息，点击【确定】保存。

#### 删除用户

从用户列表删除用户。操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择待删除的记录，点击【删除】按钮。
2. 在提示窗口，点击【确定】保存。

|  |
| --- |
| 注意：  删除某个用户时，将同时删除该用户保存的报表。 |

#### 密码重置

当用户密码丢失且无法恢复时，可通过密码重置功能为用户分配新密码。重置密码后，用户的新密码将会发送到用户注册时登记的邮箱!

操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择需要密码重置的用户，点击【重置密码】按钮。
2. 在提示窗口，点击【确定】保存。

#### 用户查询

系统提供按“用户名”、“姓名”、“备注”、“角色”、“用户来源”的模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“用户管理”菜单，查询条件中输入“用户名”、或“姓名”、或“备注”、或“角色”、或“用户类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 角色管理

**管理系统用户的所属角色，为角色分配用户和权限。提供新建角色、修改角色、删除角色功能。**

**系统中内置三种默认角色：系统管理员（sysadmin）、安全管理员（secadmin）、安全审核员（adtadmin）。**

* 系统管理员

**此角色提供对系统管理中“系统”模块及相关菜单选项的访问权限。系统管理员的操作权限有：查看状态模块的“系统信息”**、**“系统状态”**、**“系统告警”等信息；管理系统内的组织资源、用户管理、认证设置、告警管理、数据备份/恢复、许可管理、基本设置、网络管理等信息。**

**注意，系统管理员角色中的用户不具备查看详细的事件信息或创建策略等操作权限。**

* 安全管理员

**安全管理员可以配置规则、策略，跟踪事件、报表统计分析、风险趋势做出响应分析等。**

**此角色授予用户管理业务资源、**物理资源**、**数据资源**、高级资源、**规则**、网络**防护策略、网络防护规则管理、网络防护事件**、网络防护**报表**、**任务中心**等模块及相关菜单选项的访问的权限。**

* 安全审核员

**安全审核员提供对系统中“审计”模块、角色管理模块及相关菜单选项的访问权限，此角色中的用户可以查看系统告警信息。**

#### **新建角色**

操作步骤如下：

1. 选择“系统”>“角色管理”菜单，点击【新建】按钮。
2. 在“系统”>“角色管理”>“角色信息”页面，按指定要求输入信息，以及选择要定义的使用和管理权限，点击【确定】保存。

* 角色名称：角色的名称。
* 角色描述：角色的简要描述说明。
* 权限：指定该角色所要授予的访问和使用权限。

#### 编辑角色

用于修改角色信息。操作步骤如下：

1. 选择“系统”>“角色管理”菜单，选择待编辑的记录，点击“修改”按钮。
2. 在“系统”>“用户管理”>“角色信息”页面，按指定要求输入信息，并勾选所需要访问权限的模块，点击【确定】保存。

#### 删除角色

用于删除角色信息。操作步骤如下：

1. 选择“系统”>“角色管理”菜单，选择待删除的记录，点击【删除】按钮。
2. 在“确定要删除已选择的角色吗?”提示窗口，点击【确定】按钮。

|  |
| --- |
| 注意：   * 当存在用户与角色相关联时，不允许删除该角色。 * 系统预定义的角色不可删除。 |

#### 角色查询

系统提供按“角色名称”、“角色描述”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“角色管理”菜单，查询条件中输入“角色名称”、或“角色描述”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 认证设置

用于活动目录管理服务器的设定，在“网络用户”校验时使用，正确配置后，会在“网络用户”页面中显示用户信息。

操作步骤如下：

1. 选择“系统”>“认证设置”菜单；

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 名称 | 域控服务器的名称。 |
| 地址/主机名 | 域控服务器的IP地址或主机名称。 |
| 端口 | 用户目录服务器的端口号，默认为389。 |
| 用户名 | 可以访问用户目录服务器的用户名。列表。 |
| 密码 | 上述用户名的密码。 |
| 默认搜索范围  （可选） | 输入用于搜索域用户信息的搜索范围。输入的值在域中必须是正确的可识别名称（DN）。若该值为空，则从目录服务器的最上层开始搜索。 |

1. 在 “认证设置”页面，按指定要求输入信息，以及选择要定义的认证方式，点击【确定】保存。

### 数据备份/恢复

系统提供“业务数据”、“安全数据”、“配置数据”和“系统数据”的备份、恢复功能。

“业务数据”：指系统的业务信息，包括业务资源、物理资源、数据资源、高级资源、规则、规则组、策略、网络防护报表等信息。

“安全数据”：指生成的安全审计事件信息。

“配置数据”：指系统配置信息，包括组织资源、用户管理、角色管理、认证管理、基本设置、许可管理、隔离区设置等信息。

“系统数据”：指业务数据、安全数据、配置数据、已部署到本地的策略、高级资源等文件信息。文件下载后，打开此文件时需要密码。密码信息请联系管理员。

数据归档操作步骤如下：

1. 选择“系统”>“数据备份/恢复”菜单。
2. 选择需要备份的数据类别，点击左上方【归档】。

数据恢复操作步骤如下：

1. 选择“系统”>“数据备份/恢复”菜单。
2. 点击右侧的【恢复】按钮，选择需要恢复的数据文件，点击【恢复】按钮。
3. 点击右侧的【下载】按钮,可以把相关的数据文件下载到本地。
4. 点击右侧的【删除】按钮, 连同前后台记录一并删除。

### 告警管理

点击“系统”>“告警管理”菜单，“告警管理”页面会向用户显示系统告警信息， “告警管理”分为“历史告警”、“实时告警”和“告警统计”三个功能模块。

|  |
| --- |
| 注：  系统告警管理仅供系统管理员用户使用。 |

#### 历史告警

历史告警显示历次系统告警信息，告警信息最多显示最近10万条记录，超出10万限制，系统删除最早的记录。

* 告警名称：显示当前记录的告警名称，包括CPU告警、内存告警、存储告警。
* 告警类型：显示当前记录的告警类型，包括系统告警。
* 系统告警：指CPU、内存、存储告警、登陆异常告警。
* 告警级别：告警级别分为提示、一般、严重、重要、紧急五类。
* 提示：当CPU、内存、存储达到指定阈值，触发提示告警。
* 一般：当CPU、内存、存储达到指定阈值，触发一般告警。
* 严重：当CPU、内存、存储达到指定阈值，触发严重告警。
* 重要：当CPU、内存、存储达到指定阈值，触发重要告警。
* 紧急：当CPU、内存、存储达到指定阈值，触发紧急告警。
* 捕获时间：显示触发告警的具体时间。
* 告警描述：显示告警记录的描述内容及解除告警的办法。
* 告警状态：显示告警是否已被管理员确认。
* 操作：对告警进行确认操作。
* 告警详细信息：显示告警记录的详细内容，内容包括告警名称、告警级别、告警触发条件、告警捕获时间、告警描述。

#### 实时告警

实时告警显示当前时间最近的15条告警信息。

* 告警名称：显示告警类型，包括CPU告警、内存告警、存储告警。
* 告警级别：告警级别分为提示、一般、严重、重要、紧急五类。
* 提示：当CPU、内存、存储达到指定阈值，触发提示告警。
* 一般：当CPU、内存、存储达到指定阈值，触发一般告警。
* 严重：当CPU、内存、存储达到指定阈值，触发严重告警。
* 重要：当CPU、内存、存储达到指定阈值，触发重要告警。
* 紧急：当CPU、内存、存储达到指定阈值，触发紧急告警。
* 捕获时间：显示触发告警的具体时间。
* 告警描述：显示告警记录的描述内容及解除告警的办法。
* 告警状态：显示告警是否已被管理员确认。
* 操作：对告警进行确认操作。
* 告警详细信息：显示告警记录的详细内容，内容包括告警名称、告警级别、告警触发条件、告警捕获时间、告警描述。

|  |
| --- |
| 注：  【确认】某告警信息，此信息就不会在‘历史告警’、‘实时告警’列表中展现，但会在‘告警统计’中统计 |

#### 告警统计

告警统计能够根据条件显示告警趋势图。

* 告警统计条件：
* 告警级别：告警级别分为提示、一般、严重、重要、紧急五类，支持全选或多选。
* 告警状态：告警状态分为“确认”和“未确认”两种。
* 告警触发条件：选择告警统计的分组方式，例如： CPU、内存、存储。
* 时间粒度：选择告警统计的时间粒度，例如：最近一月、最近一周、天、自定义。当选择自定义时，系统显示起始时间、结束时间页面。

起始时间：统计告警信息的起始时间。

结束时间：统计告警信息的结束时间。

* 查询：根据定义的起始时间显示告警趋势图。
* 重置：重置告警统计条件。

#### 告警查询

系统提供按“告警名称”、“告警描述”、 “告警级别”、“捕获时间”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“告警管理”菜单，在“历史告警”选项卡或“实时告警”选项卡中，查询条件中输入“告警名称”、或“告警描述”、或“告警级别”、或“捕获时间”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 告警阈值设置（系统告警阈值设置）

提供触发系统告警阈值设置。

系统阈值告警分为：CPU峰值设置、内存峰值设置、磁盘峰值设置三类。每类系统告警阈值设置中，如果同时勾选多个告警级别的阈值设置，则触发最高级别的系统告警（峰值越高，级别越高）。页面截图及内容说明如下：



* CPU峰值设置：当CPU使用率达到指定百分比时，触发相应级别的CPU告警，例如：勾选“紧急：>=90”,当CPU使用率达到90%时，触发“紧急CPU告警”；不勾选此项，表示不需触发CPU系统告警。
* 内存峰值设置：当内存使用率达到指定百分比时，触发相应级别的内存告警，例如：勾选“紧急：>=90”,当内存使用率达到90%时，触发“紧急内存告警”；不勾选此项，表示不需触发内存系统告警。
* 磁盘峰值设置：当磁盘使用率达到指定百分比时，触发相应级别的磁盘告警，例如：勾选“紧急：>=90”,当磁盘使用率达到90%时，触发“紧急磁盘告警”；不勾选此项，表示不需触发磁盘系统告警。

### 许可管理

用于管理系统许可密钥。根据购买协议确定系统使用许可。

上传许可文件，操作步骤如下：

1. 选择“系统”>“许可管理”菜单。
2. 在“许可管理”上传证书页面点击【选择】按钮选择有效的“license文件”，点击【确定】按钮保存。

### 日志服务器设置

用于系统日志的上传设置，进行统一归档处理。

操作步骤如下：

1. 选择“系统”>“日志服务器设置”菜单。
2. 在“日志服务器设置”页面，指定要求输入信息，以及选择要定义的认证方式，点击【确定】保存。

* 是否传输：上传日志功能启用与否；
* 日志服务器地址：收集日志的服务器IP地址；
* 服务器端口：日志传输所用的UDP端口；
* 优先级：上传日志的优先级；
* 传输类型：日志传输的类型；
* 日志类型：需要上传的日志类型。

### 基本设置

用于管理系统各类参数的设定。此章节包括以下内容：

* 邮件服务器设置
* 时间设置

#### **邮件服务器**

用于发送告警或报表计划时所用的邮件服务器设定。

操作步骤如下：

1. 选择“系统”>“基本设置”菜单。
2. 在“基本设置”页面，选择“邮件服务器”选项卡，按指定要求输入信息，以及选择要定义的认证方式，点击【确定】保存。

* SMTP服务器：发送邮件告警、报表计划和事件上报时所用的邮件服务器地址。
* SMTP服务器端口：发送告警或计划时所用的邮件服务器端口，默认端口为25。
* 邮件地址：用于发送告警或计划时发件人的邮箱地址。
* 密码：用于发送告警或计划时发件人的邮箱密码。

#### **时间设置**

设置系统日期和时间。

操作步骤如下：

1. 选择“系统”>“基本设置”菜单。
2. 在“基本设置”页面，选择“时间设置”选项卡，按指定要求输入信息，点击【确定】保存。

### 升级管理

系统提供软件系统升级功能。

#### 上传升级包

操作步骤如下：

1. 选择“系统”>“升级管理”菜单，点击【服务端升级管理】选项卡。
2. 点击【上传】按钮，点击【选择】按钮，选择正确的升级包文件（.tar.gz格式，且小于500M）。
3. 点击【上传】按钮，直至升级包上传成功。
4. 上传成功后，服务端升级管理列表，升级包记录状态显示为“未部署”，且“上传时间”正确显示。

#### 部署升级包

操作步骤如下：

1. 服务端升级管理列表，选择待升级的记录，点击【升级】按钮，直至升级成功。
2. 期间系统提示“升级成功，服务端正在重启，请稍后在服务器升级管理中查看状态”，点击【确定】按钮退出提示框。

注意：升级完成后设备会自动重新启动，需待设备完全启动成功后方可继续使用。

1. 待设备启动成功后，重新登录系统，选择“系统”>“升级管理”菜单，点击【服务端升级管理】选项卡，查看服务端升级管理列表，升级包记录状态显示为“已部署”，且“升级时间”正确显示。

#### 删除升级包

操作步骤如下：

1. 服务端升级管理列表，选择待删除的记录，点击【删除】按钮。
2. 系统提示“未应用该升级包的服务端将无法升级。确定要删除已选择的服务端升级包吗?”，点击【确定】按钮，确定删除。

系统支持批量删除和单条记录删除。

### 信任主机管理

“信任主机”是指可以访问系统的主机，如不在信任主机列表的主机将不允许访问系统。

#### 新建信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，点击【信任主机添加】选项卡。
2. 在“信任主机列表”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 名称 | 信任主机的名称 |
| 主机IP | 信任主机的IP地址 |

#### 编辑信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，选择待编辑的信任主机。
2. 在该记录的最右侧点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，选择待删除的信任主机记录。
2. 点击该记录右侧的【🗑删除】按钮，在提示窗口，点击【确定】保存。

#### 信任主机模糊查询

系统提供按“名称”、“信任IP”、“备注”模糊查询功能。

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，查询条件中输入“名称”、“信任IP”、“备注”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 网络管理

网络管理提供系统相关网络设置。

#### 工作模式

首先需要对系统工作模式进行选择之后，然后数据才可以通过正确的方式进行审计。

系统的工作模式分为旁路模式和串接模式。

旁路模式：不影响用户网络架构的部署模式。

* 串接模式：嵌入用户网络架构的部署模式。
* 网桥模式：设备透明的对流量进行审计的模式。
* 路由器模式：设备作为网关，对流量进行转发的模式。

还需要对以下进行设置：

* 光口：通过光纤线缆来进行数据传输，接口模块一般为sfp(传输率2gb/s)和gbic(1gb/s),对应的接口为sc和lc。
* 电口：通过光纤线缆来进行数据传输，接口模块一般为sfp(传输率2gb/s)和gbic(1gb/s),对应的接口为sc和lc。
* 设置VLANID:输入VLANID值，多个VLANID是以空格进行分割，点击【提交】确定。

##### 新建工作模式

操作步骤如下：

1. 选择“系统”>“网络管理”>菜单，在“工作模式”选项中，点击【添加】按钮。
2. 在 弹出页面，按指定要求输入信息，点击【提交】保存。

* 旁路模式下需要输入信息如下：
* 接口名：输入接口名称。
* IP地址：输入IP地址。
* 网桥模式下需要输入信息如下：
* 网桥名：输入网桥名称。
* 网络地址：输入网络地址。
* 网络掩码：输入网络掩码。
* 网关地址：输入网关地址。
* 路由模式下需要输入信息如下：
* 入口地址：输入入口地址。
* 入口掩码：输入入口掩码。
* 入口网关：输入入口网关。
* 出口地址：输入出口地址。
* 出口掩码：输入出口掩码。
* 出口网关：输入出口网关。

##### 编辑工作模式

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“工作模式”选项卡中，选择待编辑的记录。
2. 点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除工作模式

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“工作模式”选项卡中，选择待删除的记录。
2. 点击【删除】按钮，在提示窗口，点击【确定】保存。

##### 提交

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“工作模式”选项卡中，选择待提交的记录。
2. 点击【提交】按钮进行提交。

##### 刷新

系统提供界面的刷新功能。

具体操作：选择“系统”>“网络管理”菜单，在“工作模式”选项卡中，点击【刷新】按钮，即可将界面进行更新。

#### 网络接口

##### 新建网络接口

操作步骤如下：

1. 选择“系统”>“网络管理”>菜单，在“网络接口”选项中，选择待添加的主接口，点击【添加】按钮。
2. 在弹出页面，按指定要求输入信息，点击【提交】保存。

##### 编辑网络接口

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“网络接口”选项卡中，选择待编辑的记录。
2. 点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除网络接口

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“网络接口”选项卡中，选择待删除的记录。
2. 点击【删除】按钮，在提示窗口，点击【确定】保存。

#### 路由设置

##### 新建路由

操作步骤如下：

1. 选择“系统”>“网络管理”>菜单，在“路由设置”选项中，点击【添加】按钮。
2. 在弹出页面，按指定要求输入信息，点击【提交】保存。

* 路由类型：选择所需的路由类型，包括两种：静态路由和策略路由。
* 静态路由：是基于数据包目的地址向指定的下一个跳转发数据包。
* 策略路由：是基于数据包源地址包头中的其他域向指定的下一跳转发数据包。
* 源子网IP:输入源子网IP地址；
* 源子网掩码：输入源子网掩码；
* 目的子网：输入目的子网；
* 目的子网掩码：输入目的子网掩码；
* 网关：输入网关地址；
* 网络接口：选择网络接口；
* 状态：是指添加路由的状态，包含停用和启用两种。
* 停用：选择此项，代表添加路由为停用状态；
* 启用：选择此项，代表添加路由为启用状态；

注意：

因为不同的路由类型需要输入的信息不同，因此，需要根据选择的路由类型进行相应的信息内容输入。

##### 编辑路由

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“路由设置”选项卡中，选择待编辑的路由。
2. 点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除路由

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“路由设置”选项卡中，选择待删除的路由。
2. 点击【删除】按钮，在提示窗口，点击【确定】保存。

##### 启用

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“路由设置”选项卡中，选择待启用的路由。
2. 点击【启用】按钮，进行路由的启用操作。

##### 停用

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，在“路由设置”选项卡中，选择待停用的路由。
2. 点击【停用】按钮，进行路由的停用操作。

#### DNS设置

操作步骤如下：

1. 选择“系统”>“网络管理”菜单，选择“DNS设置”选项卡。
2. 在“DNS设置”选项卡中，输入要求输入的信息，点击【提交】按钮进行保存。

* 首选DNS服务器：输入首选DNS服务器的IP地址；
* 备用DNS服务器一：输入备用DNS服务器一的IP地址；
* 备用DNS服务器二：输入备用DNS服务器二的IP地址。

## 安全管理员

系统提供基于安全管理员角色的访问控制权限，作为安全管理员，具备以下权限：

* 状态查看：查看 “24小时TOP5服务/客户端IP事件数总览”等信息。
* 管理资源：管理与数据相关的“业务资源”、“地理映射”。
* 物理资源：管理系统要检测的主机资源、网络资源。
* 数据资源： 管理系统检测结构化或非结构化数据内容的特征，例如：“文档特征”、“关键字”、“关键字组”、“匹配模式”、“文档指纹”、“数据库指纹”、“二维智能学习”等。
* 规则：管理执行扫描策略时用的匹配规则，例如 “发现扫描规则”。
* 策略：管理发现扫描制定的策略，例如“网络防护策略”、“网络防护全局设置”。
* 事件管理：用于管理和维护安全事件，例如：“网络防护事件”。
* 报表管理：用于管理和维护报表，例如：“全局状态设置”、“报表计划任务”、“全球数据态势感知”、“报表风格设置”、“网络防护报表”。
* 任务中心：显示高级资源任务的执行信息，例如：执行任务的起止时间、执行进度、执行结果、总大小、已处理、未处理文件等信息。
* 权限管理：创建系统管理用户、角色及权限，例如：个人中心、用户管理、角色管理。
* 数据管理：管理与维护系统数据，例如：日志维护。
* 系统设置：管理系统基本配置，例如：密码安全策略设置、信任主机管理。

**操作流程如下：**

1. 创建“业务资源”。
2. 创建“物理资源”，创建以下物理资源：

* 创建“主机资源”。
* 创建“主机资源组”。
* 创建“网络资源”。

1. 创建“数据资源”，创建以下数据资源：

* 创建“文档特征”资源。
* 创建“关键字”资源。
* 创建“关键字组”资源。
* 创建“匹配模式”资源。

1. 创建“高级资源”，创建以下高级资源：

* 创建“文档指纹”资源。
* 创建“数据库指纹”资源。
* 创建“二维智能学习”资源。

1. 创建“规则”。
2. 创建“规则组”。
3. 创建“策略”。
4. 【部署】策略。
5. “任务中心”查看任务的执行情况。
6. “网络防护报表”，统计和管理发现事件报表报表。

|  |
| --- |
| 注意：   * “数据资源”或“高级资源”、“规则”、“规则组”、“策略”在编辑后，需要重新部署。 * “数据资源”或“高级资源”被“规则”引用时，不允许删除。 |

以下将对上述功能分别进行描述

### 查看系统状态

安全管理员（secadmin）登录系统后，选择“状态”菜单，进入状态视图，此页面可查看 “24小时TOP5服务IP事件数总览”、“24小时TOP5客户端IP事件数总览”以及“自定义首页报表”。

24小时TOP5服务IP事件总览：以饼图形式显示前五个（正序）TOP5服务IP事件数量。

24小时TOP5客户端IP事件总览：以饼图形式显示前五个（正序）TOP5客户端IP事件数量。

网络防护按照部门业务统计：以饼图形式按照部门业务种类统计事件数量。

### 业务资源管理

业务资源是将企业内部待防护的数据资产根据“业务类型”进行分类，业务资源可以归属于企业内的某个组织资源，组织资源可以理解为“部门”。例如，“市场部的市场企划案”或者“财务部的财务报表”均可定义为业务资源。

#### 新建业务资源

添加新的业务资源。操作步骤如下：

1. 选择“首页”>“资源”>“业务资源”菜单；
2. 点击【业务添加】按钮,按指定要求输入信息，点击【确定】按钮保存。

* 业务名称：输入业务资源的名称。
* 规则组：指定业务数据所要引用的发现扫描规则组。
* 选择关联组织：指定该业务资源对应的“部门”，即“组织资源”。

#### 编辑业务资源

修改业务资源信息。操作步骤如下：

1. 选择“首页”>“资源”>“业务资源”菜单；
2. 在“业务列表”中，选择需要编辑的记录，点击最右侧操作中的【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除业务资源

删除业务资源信息。操作步骤如下：

1. 选择“首页”>“资源”>“业务资源”菜单；
2. 在“业务列表”中，选择要删除的记录，点击记录最右侧操作栏内的【删除】按钮，弹出提示窗口，点击【确定】删除。

#### 业务资源模糊查询

系统提供按“业务名称”、“备注”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“业务资源”菜单，在“业务列表”选项卡中，查询条件中输入“业务名称”、或“备注”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 地理映射

地理映射是将企业内部地址与地理区域向对应，将网络防护事件在“数据态势感知”中进行可视化展现。

#### 新建地理映射

添加新的地理映射。操作步骤如下：

1. 选择“首页”>“资源”>“地理映射”菜单；
2. 点击【新建】按钮,按指定要求输入信息，点击【确定】按钮保存。
   * + \*名称：输入共享目录主机资源的名称。
     + 备注：网络资源的描述信息。
     + \*ip：需要映射的IP地址。
     + \*网段/掩码：需要映射的IP地址段/掩码。
     + \*IP区间：需要映射的IP区间。
     + \*省：IP被映射到的省份。
     + \*市：IP被映射到的市。
     + \*县/区：IP被映射到的区县。

#### 编辑地理映射

修改地理映射信息。操作步骤如下：

1. 选择“首页”>“资源”>“地理映射”菜单；
2. 在“地理映射”中，选择需要编辑的记录，点击最右侧操作中的【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除地理映射

删除地理映射信息。操作步骤如下：

1. 选择“首页”>“资源”>“地理映射”菜单；
2. 在“地理映射”中，选择要删除的记录，点击记录最右侧操作栏内的【删除】按钮，弹出提示窗口，点击【确定】删除。

#### 地理映射的模糊查询

系统提供按“名称”、“类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“地理映射”菜单，在“地理映射”选项卡中，查询条件中输入“名称”、或“类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 主机资源管理

系统支持按“数据源类型”将需要扫描数据的目标主机资源进行分类。例如，共享目录主机资源、数据库主机资源。

以上数据源中可能包含敏感数据。为防止敏感数据外泄，将目标主机资源作为扫描目标执行发现扫描策略。

使用主机资源时，必须具备访问被扫描主机资源的权限，读取权限说明如下所示：

* 共享目录主机资源

具备扫描“共享用户的文件”的读取权限。

* 数据库主机资源
* Mysql数据库

需同时满足以下几个条件：

1. 具备访问information\_schema.SCHEMATA表的权限。
2. 具备访问information\_schema.TABLES表的权限。
3. 具备“被扫描数据库的Select语句权限”。
4. 被扫描数据库的数据格式必须为utf-8编码格式：SET NAMES utf-8。

* Oracle数据库

需同时满足以下几个条件：

1. 具备访问DBA\_USERS/USER\_TABLES表的权限。
2. 具备“被扫描用户的用户数据表Select语句权限”。

* Mssql数据库

需同时满足以下几个条件：

1. 具备访问SYS.DATABASES表的权限。
2. 同时具备“被扫描数据库的Select语句权限”。

#### 新建主机资源

添加新的主机资源。操作步骤如下：

* 新建共享目录主机资源
  1. 进入“首页”>“资源”>“主机资源”，点击【新建】。
  2. 点击【共享目录】选项卡下，输入相关信息，点击【确定】完成创建。
     + \*名称：输入共享目录主机资源的名称。
     + \*IP地址：选择或输入共享目录主机资源的IP地址。
     + 备注：输入共享目录主机资源的备注。
     + 计算机全名：输入共享目录的计算机的全名。
     + 加入主机组：将共享目录主机资源加入已经创建的主机资源组内。
     + \*用户名：输入能够访问共享目录主机资源的用户名。
     + \*密码：输入该用户名的密码。
     + \*确认密码：再次输入该用户名的密码。
     + 域名：如果该主机资源为域内的计算机，则输入域名。
     + 测试链接：输入完成IP地址以及用户名、密码后可点击测试链接查看该认证信息与IP地址是否匹配，如果显示链接成功，则说明认证信息正确。
     + 新建：为主机资源新建目标资源组，可选择该主机资源中已共享一个或者多个目录作为一个目标资源组。
* 数据库主机资源
  1. 进入“首页”>“资源”>“主机资源”，点击【新建】。
  2. 在【数据库】选项卡下，输入相关信息，点击【确定】完成创建。
     + \*名称：输入数据库主机资源的名称。
     + \*数据库类型：选择数据库主机资源的数据库类型。
     + \*IP地址：选择或输入数据库主机资源的IP地址。
     + 备注：输入数据库主机资源的备注。
     + 计算机全名：输入数据库主机资源所属的计算机全名。
     + \*端口：输入数据库主机资源所使用的端口。

Mysql数据库默认端口号为3306；

Oracle数据库默认端口号为1521；

SqlServer数据库默认端口号为1433；

* + - \*用户名：输入能够访问数据库主机资源的用户名，需具备可读权限。
    - \*密码：输入用户名所对应的密码。
    - \*确认密码：再次输入用户名的密码。
    - \*数据库：选择待扫描数据库服务器的数据库名称。
    - 域名：如果主机资源加入域，则需要输入域名。
    - 是否全库扫描：勾选此项，表示执行扫描策略时对全库进行扫描。
    - 测试链接：输入以上信息，点击【测试链接】按钮可验证以上认证信息与IP地址是否匹配，如果显示链接成功，则说明认证信息正确。
    - 新建：为数据库主机资源新建目录资源组，可以选择数据库中的部分表作为扫描目标。

#### 编辑主机资源

编辑主机资源信息。操作步骤如下：

1. 选择“首页”>“资源”>“主机资源”菜单。
2. 选择【主机资源】选项卡，选择需要编辑的主机资源，点击该主机资源最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除主机资源

删除主机资源信息。操作步骤如下：

1. 选择“首页”>“资源”>“主机资源”菜单。
2. 选择【主机资源】选项卡，选择需要删除的主机资源，点击该主机资源最右侧操作栏内的【🗑删除】按钮，弹出提示窗口，点击【确定】删除主机资源。

#### 主机资源模糊查询

系统提供按“名称”、“IP地址”、“资源类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“主机资源”菜单，在“主机资源”选项卡中，查询条件中输入“名称”、或“IP地址”、或“资源类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 新建主机资源组

添加新的主机资源组。操作步骤如下：

1. 选择“首页”>“资源”>“主机资源”菜单。
2. 选择【主机资源组】选项卡，点击【新建】。按指定要求输入信息，点击【确定】保存。

* 名称：输入主机资源组的名称。
* 备注：可输入该主机资源组的备注信息。
* 主机资源：将备选列表中的资源加到成员列表。（注：只能选择同样类型的资源，根据【资源类型】处进行过滤）。

#### 编辑主机资源组

编辑主机资源组信息。操作步骤如下：

1. 选择“首页”>“资源”>“主机资源”菜单。
2. 选择【主机资源组】选项卡，选择需要编辑的主机资源组，点击该主机资源组最右侧操作栏下的【修改】，按指定要求输入信息，点击【确定】保存。

#### 删除主机资源组

删除主机资源组信息。操作步骤如下：

1. 选择“首页”>“资源”>“主机资源”菜单。
2. 选择【主机资源组】选项卡，选择需要删除的主机资源组，点击该主机资源组最右侧的操作栏内的【🗑删除】按钮，弹出提示窗口【确定】删除。

#### 主机资源组模糊查询

系统提供按“名称”、“资源类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“主机资源”菜单，在“主机资源组”选项卡中，查询条件中输入“名称”、或“资源类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 网络资源管理

用于管理可能存储敏感数据的网络目标资源，例如某个网段、某个IP地址区间的网络路径，系统支持根据网段、IP地址区间定义扫描目标。

#### 新建网络资源

添加新的网络资源，操作步骤如下：

1. 选择“首页”>“资源”>“网络资源”菜单。
2. 点击【新建】。输入相关信息，点击【确定】保存。

* 名称：网络资源的名称。
* 备注：网络资源的描述信息。
* 类型：选择网络资源类型，表明该网络资源的属性，以下属性可以选择一种。
* 网段：网段信息，并且填写该网段的掩码。
* IP区间：划分具体IP地址区间。

#### 编辑网络资源

编辑网络资源，操作步骤如下：

1. 选择“首页”>“资源”>“网络资源”菜单。
2. 选择一条要编辑的记录，点击该网络资源最右侧操作栏下的【修改】按钮，输入相关信息，点击【确定】按钮保存。

#### 删除网络资源

删除网络资源信息。操作步骤如下：

1. 选择“首页”>“资源”>“网络资源”菜单。
2. 选择需要删除的网络资源，点击该网络资源最右侧操作栏内的【🗑删除】按钮，弹出提示窗口，点击【确定】删除。

#### 网络资源模糊查询

系统提供按“名称”、“资源类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“网络资源”菜单，在“网络资源”选项卡中，查询条件中输入“名称”、或“资源类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 数据资源管理

本节描述以下资源：

* 文档特征
* 关键字
* 匹配模式

#### 文档特征

管理文档特征相关的内容资源，文档特征资源可以是“文档类型”、“文档名称”。

##### 新建文档类型

文档类型资源可以包含一个或者多个文件扩展名（\*.doc），比如创建的文档类型资源为\*.doc。

操作步骤如下：

1. 选择“资源”>“文档特征”菜单。
2. 在“资源”>“文档特征”页面中，点击【文档类型】选项卡下的【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入该文档资源的名称。
* 备注：输入该文档资源的备注信息。
* 类型：选择待扫描目标资源的文档类型。
* 过滤：用于搜索文档类型，输入文档类型或名称，点击按钮即可。

##### 编辑文档类型

操作步骤如下：

1. 选择“资源”>“文档特征”菜单。
2. 在“资源”>“文档特征”页面的【文档类型】选项卡中，选择一条要编辑的记录，点击该记录最右侧的操作栏下的【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除文档类型

操作步骤如下：

1. 选择“资源”>“文档特征”菜单。
2. 在“资源”>“文档特征”页面的【文档类型】选项卡中，选择一条要删除的记录，点击该记录最右侧操作栏内（或操作栏上方）的【删除】按钮，弹出提示窗口点击【确定】删除。系统支持批量删除和单条记录删除。

##### 新建文档名称

用于添加新的“文档名称”资源。此资源通过文件扩展名鉴别文件。文件名称资源可以包含一个或者多个文件名称，比如创建的资源为名称A。

操作步骤如下：

1. 选择“资源”>“文档特征”菜单。
2. 在“资源”>“文档特征”页面中，点击文档名称选项卡下的【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入该文档资源的名称。
* 备注：输入该文档资源的描述信息。
* 文件名：指定该资源的文件名称。
* 【增加】按钮：用于在该资源中增加新的文件名。可以一次增加多个文件名。
* 【删除】按钮：用于删除已有列表的文件名。

##### 编辑文档名称

用于编辑文档名称资源，操作步骤如下：

1. 选择“资源”>“文档特征”菜单。
2. 在“资源”>“文档特征”页面的【文档名称】选项卡中，选择需要编辑的记录，点击该记录最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除文档名称

用于删除文档名称资源，操作步骤如下：

1. 选择“资源”>“文档特征”菜单。
2. 在“资源”>“文档特征”页面的【文档名称】选项卡中，选择一条要删除的记录，点击该记录最右侧操作栏内的【删除】按钮，弹出提示窗口，点击【确定】删除。

##### 文档特征模糊查询

系统提供按“名称”、“备注”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“文档特征”菜单，在“文档类型”或“文档名称”选项卡中，查询条件中输入“名称”、或“备注”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 关键字

用于管理关键字资源，关键字资源是指定系统要处理含有关键字的文件，当扫描目标文件内容中含有指定的关键字时，关键字资源激活。

##### 新建关键字资源

添加新的关键字资源。操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字”页面中，点击【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入该关键字资源的名称。
* 关键字：输入关键字短语。
* 是否精确匹配：检测关键字是否需要精确匹配。
* 备注：输入该关键字资源的描述信息。

##### 编辑关键字资源

编辑关键字资源，操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字”页面中，选择需要编辑的关键字，点击该关键字最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除关键字资源

删除关键字资源，操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字”页面中，选择需要删除的关键字，点击该关键字最右侧操作栏内的【删除】按钮，弹出提示窗口点击【确定】删除。

##### 导入关键字资源

导入关键字资源，操作步骤如下：

操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字”页面中，点击【导入】按钮，选择需要导入的关键字文件，点击【导入】进行关键字资源的导入。

##### 关键字模糊查询

系统提供按“名称”、“关键字”、“备注”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“关键字”菜单，在“关键字”选项卡中，查询条件中输入“名称”、或“关键字”、或“备注”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 关键字组

关键字组资源是若干个关键字的集合，可包含多个关键字。同时系统提供预定义关键字组，每个预定义关键字组涵盖了一个相关行业的敏感数据内容，通过派生的方式在预定义关键字组基础上进行编辑生成新的关键字组数据资源，也可以创建新的关键字组数据资源。

##### 预定义关键字组派生

操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字”页面中，点击关键字组选项卡，选择将派生的预定义关键字组记录，点击【派生】按钮，根据需求增加或删除关键字短语，并按指定要求输入信息，点击【确定】保存。

* 名称：输入该关键字组资源的名称。
* 备注：输入该关键字组资源的描述信息。
* 包含的关键字列表：输入关键字组包含的关键字短语。关键字短语区分大小写。
* 是否精确匹配：检测关键字是否需要精确匹配。
* 权重：为每个关键字短语输入从 1 到999的权重。当权重与某个阀值匹配时，会定义触发某个策略所必须找到的关键字短语实例的数目（相对于其他关键字短语）。默认情况下，关键字短语权重指定为1。

例如：如果阀值为设为100，而关键字短语权重为10，假如不匹配其他关键字短语，如果扫描目标文件中包含该关键字短语的9个实例，超出此数目才会触发某个策略。如果关键字短语A的权重为10，而关键字短语B的权重为5，则关键字短语A的5个实例以及关键字短语B的10个实例将触发该策略。如果有排除关键字短语，系统会减去已排除的关键字短语的权重。

* 【增加】按钮：用于在该资源中增加新的关键字短语。关键字组资源可以添加多条关键字关键字短语。
* 【删除】按钮：用于删除已有列表的关键字关键字短语。

##### 新建关键字组资源

添加新的关键字组资源。操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字”页面中，点击关键字组选项卡下方的【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入该关键字组资源的名称。
* 备注：输入该关键字组资源的描述信息。
* 包含的短语列表：输入关键字组包含的关键字短语。关键字短语区分大小写。
* 是否精确匹配：检测关键字是否需要精确匹配。
* 权重：为每个关键字短语输入从 1 到999的权重。当权重与某个阀值匹配时，会定义触发某个策略所必须找到的关键字短语实例的数目（相对于其他关键字短语）。默认情况下，关键字短语权重指定为1。

例如：如果阀值为设为100，而关键字短语权重为10，假如不匹配其他关键字短语，如果扫描目标文件中包含该关键字短语的9个实例，超出此数目才会触发某个策略。如果关键字短语A的权重为10，而关键字短语B的权重为5，则关键字短语A的5个实例以及关键字短语B的10个实例将触发该策略。如果有排除关键字短语，系统会减去已排除的关键字短语的权重。

* 【导入】按钮：用于在该资源中导入新的关键字短语。
* 【增加】按钮：用于在该资源中增加新的关键字短语。关键字组资源可以添加多条关键字关键字短语。
* 【删除】按钮：用于删除已有列表的关键字关键字短语。

##### 编辑关键字组资源

用于编辑关键字组资源，操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字组”选项卡中，选择一条要编辑的关键字组，点击该关键字组最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除关键字组资源

删除关键字组资源，操作步骤如下：

1. 选择“资源”>“关键字”菜单。
2. 在“资源”>“关键字组”选项卡中，选择需删除的关键字组，点击该关键字组最右侧操作栏内的【删除】按钮，弹出提示窗口点击【确定】删除。

##### 关键字组模糊查询

系统提供按“名称”、“备注”、“类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“关键字”菜单，在“关键字组”选项卡中，查询条件中输入“名称”、或“备注”、或“类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 匹配模式

管理匹配模式资源，匹配模式资源定义要在内容中搜索的模式，以及设置查找此类模式时要采取的操作。该资源采用“正则表达式”的方式，根据某些语法规则来描述或匹配一组字符串。

同时系统提供预定义匹配模式，每个预定义匹配模式涵盖了同类敏感数据内容，通过派生的方式在预定义匹配模式基础上进行编辑生成新的匹配模式数据资源，也可以创建新的匹配模式数据资源。

##### 预定义匹配模式派生

操作步骤如下：

1. 选择“资源”>“匹配模式”菜单。
2. 在“资源”>“匹配模式”页面中，选择将派生的预定义匹配模式记录，点击【派生】按钮，根据自身需求修改正则表达式或短语，并按指定要求输入信息，点击【确定】按钮保存。

* 名称：输入该匹配模式资源的名称。
* 备注：输入该匹配模式资源的备注信息。
* 值：输入用户自定义内容的正则表达式的值（注意：只能输入一个正则表达式）。
* 排除：正则表达式的定义范围较宽泛，为了减少信息误报，可以将某些值从模式中排除。系统提供以下两种排除类型：
* 排除模式：选择此项，表示定义要排除的正则表达式模式。
* 排除短语：选择此项，表示要排除的一系列短语。

【增加】按钮：增加排除短语。可以添加多条短语。

【删除】按钮：删除排除短语列表的短语。

##### 新建匹配模式资源

添加新的匹配模式资源。操作步骤如下：

1. 选择“资源”>“匹配模式”菜单。
2. 在“资源”>“匹配模式”页面中，点击【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入该匹配模式资源的名称。
* 备注：输入该匹配模式资源的备注信息。
* 值：输入用户自定义内容的正则表达式的值（注意：只能输入一个正则表达式）。
* 排除：正则表达式的定义范围较宽泛，为了减少信息误报，可以将某些值从模式中排除。系统提供以下两种排除类型：
* 排除模式：选择此项，表示定义要排除的正则表达式模式。
* 排除短语：选择此项，表示要排除的一系列短语。

【增加】按钮：增加排除短语。可以添加多条短语。

【删除】按钮：删除排除短语列表的短语。

##### 编辑匹配模式资源

修改匹配模式资源。操作步骤如下：

1. 选择“资源”>“匹配模式”菜单。
2. 在“资源”>“匹配模式”页面中，选择需要编辑的匹配模式，点击该匹配模式最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除匹配模式资源

删除匹配资源，操作步骤如下：

1. 选择“资源”>“匹配模式”菜单。
2. 在“资源”>“匹配模式”页面中，选择需要删除的匹配模式，点击该匹配模式最右侧操作栏内的【删除】按钮，弹出提示窗口点击【确定】删除。

##### 匹配模式模糊查询

系统提供按“名称”、“备注”、“类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“匹配模式”菜单，查询条件中输入“名称”、或“备注”、或“类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 高级资源管理

本节描述以下高级资源：

* 文档指纹
* 数据库指纹
* 二维智能学习

#### 文档指纹

文档指纹是指对文档通过系统内置的算法提取唯一的特征码，用于网络防护的数据匹配。

##### 新建文档指纹资源

添加新的文档指纹资源。操作步骤如下：

1. 选择“资源”>“文档指纹”菜单。
2. 在“资源”>“文档指纹”页面中，点击【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 基本信息：
* 名称：输入文档指纹资源的名称。
* 备注：输入新建文档指纹资源的备注说明。
* 目标：选择待训练文档指纹样本的共享目录主机资源。
* 关联文档：选择待训练文档指纹样本的共享目录主机资源中的目标资源组。
* 生效时间：用于指定执行扫描任务的时间和周期。
* 单次：指定扫描任务仅执行一次。具体执行时间依据属性中的时间设置情况而定。
* 文件过滤设置：用于设置过滤条件，将不必要执行扫描的文件过滤掉，以便提高扫描效率和扫描结果准确率。过滤条件分为如下几种情况：
* 过滤类型：扫描目标文件夹按文件类型（文件扩展名）过滤掉所包含类型的相关文件。不勾选，则不进行文件类型过滤处理。

1. 包含：指定要识别文档指纹的文件类型。
2. 排除：指定要排除识别文档指纹的文件类型。

* 过滤日期：扫描目标文件按文件日期过滤。不勾选，则不进行日期过滤处理。

1. 最近：表示仅扫描最近N个月的文件。
2. 超过：表示不扫描N个月前的文件。
3. 从xx至xx：表示仅扫描某个时间段的文件。

* 过滤体积：勾选此项，扫描目标文件按文件大小过滤。不勾选，则不进行文件大小过滤处理。。

1. 文件体积上限：表示仅扫描小于文件上限值的文件。
2. 文件体积下限：表示仅扫描大于文件下限值的文件。

* 文档指纹识别方法：指定一种文档指纹识别方法。

1. 相似匹配：表示查找“目标资源内容与文件之间的相似特征”。这种方法安全性较高，它能够检测目标资源的各部分内容以及精确的文件匹配内容。
2. 精确匹配：表示将“目标资源内容与文件的特征”精确匹配。对于包含许多文件的大型目录结构，建议您首先设置精确匹配文档指纹。

##### 部署文档指纹任务

文档指纹资源任务创建完成后，需要手动部署。如果文档指纹资源未部署成功或部署后未生成文档指纹样本库，则在创建规则选择高级资源时，不能显示当前创建的文档指纹资源。

##### 编辑文档指纹资源

修改文档指纹资源。操作步骤如下：

1. 选择“资源”>“文档指纹”菜单。
2. 选择一条要编辑的记录，点击该记录最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】保存。

##### 删除文档指纹资源

用于删除文档指纹资源。操作步骤如下：

1. 选择“资源”>“文档指纹”菜单。
2. 选择需要删除的记录，点击该记录最右侧的操作栏内的【删除】按钮。
3. 在“确定要删除已选择的文档指纹资源吗?”提示窗口，点击【确定】确认删除。

##### 文档指纹模糊查询

系统提供按“名称”、“备注”、“规则中使用”、“部署状态”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“文档指纹”菜单，查询条件中输入“名称”、或“备注”、或“规则中使用”、或“部署状态”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

##### 查看文档指纹任务

文档指纹资源在执行任务期间，可通过“审计”>“任务中心”任务列表查看任务执行情况。

#### 数据库指纹

数据库指纹资源是对数据库中的表或表中的多条记录字段通过系统内置的算法提取唯一的特征码，用于网络防护的数据匹配。

数据库指纹匹配属于资源，也属于扫描任务。

##### 新建数据库指纹资源

用于添加新的数据库指纹资源。在使用数据库指纹资源前，要确保已正确配置数据源，否则该资源不能正常使用。

操作步骤如下：

1. 选择“资源”>“数据库指纹”菜单。
2. 点击【新建】按钮，按指定要求输入信息，点击【确定】按钮保存。

* 名称：输入数据库指纹资源的名称。
* 备注：输入关于新建数据库指纹资源的可选描述说明。
* 目标：选择需要进行指纹识别的数据库主机资源。
* 表信息：选择此选项，表示对所选字段进行指纹识别。

从下拉列表中，选择要生成数据库指纹的表名。

* 生效时间：用于指定执行扫描任务的时间和周期。具体使用方法请参照文档指纹匹配资源中的【生效时间】介绍。

##### 部署数据库指纹任务

数据库指纹资源任务创建完成后，需要手动部署。如果数据库指纹任务未部署成功或部署后未生成数据库指纹样本库，则在创建规则时，不能选择当前创建的数据库指纹资源。

##### 编辑数据库指纹资源

用于修改数据库指纹资源。操作步骤如下：

1. 选择“资源”>“数据库指纹”菜单。
2. 选择一条要编辑的记录，点击该记录最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】按钮保存。

##### 删除数据库指纹资源

用于删除数据库指纹资源。操作步骤如下：

1. 选择“资源”>“数据库指纹”菜单。
2. 选择一条要删除的记录，点击该记录最右侧操作栏内的【删除】按钮，弹出提示窗口，点击【确定】删除。

##### 数据库指纹模糊查询

系统提供按“名称”、“备注”、“规则中使用”、“部署状态”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“数据库指纹”菜单，查询条件中输入“名称”、或“备注”、或“规则中使用”、或“部署状态”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

##### 查看数据库指纹任务

数据库指纹资源在执行任务期间，可通过“审计”>“任务中心”任务列表查看任务执行情况。

#### 二维智能学习

二维智能学习仅用于非结构化文档数据分析，不能用于数据库或结构化的数据分析。二维智能学习可以根据用户提供的敏感的或者不敏感的样本数据示例，通过系统内置算法建立匹配模型。二维智能学习需要的样本较少，但是二维智能学习可以处理大数据量文档。

##### 新建二维智能学习

用于添加新的二维智能学习资源。操作步骤如下：

1. 选择“资源”>“二维智能学习”菜单。
2. 点击【新建】按钮，按指定要求输入信息，点击【确定】按钮保存。

* 名称：输入二维智能学习的名称。
* 描述：输入关于当前新建二维智能学习的备注说明。
* 目标：选择待训练样本的共享目录主机资源。
* 正例反例：待训练样本的正例共享目录主机资源。
* 正例反例：提供数据样本，系统会自动学习并检测相似内容。为了达到最好的学习效果，正、反例文件夹中建议示例数量为1500。
* 正例：浏览至包含保护的文本数据类型示例的文件夹，系统将学习这些示例并识别流量中的相似数据。

点击【浏览】按钮，选择需要保护的文本数据类型示例文件夹，点击【提交】按钮。

* 反例：浏览至包含相似但并非需要保护的文本数据示例的文件夹。该文件夹必须专门用于反例，且不能是正例的子目录。

点击【浏览】按钮，选择文本数据类型示例文件夹，点击【提交】按钮。

* 内容类型：下拉列表中选择最能描述想保护的内容的类型，此内容必须与正例文件夹中的内容类型相匹配。

当前系统提供一种内容类型为“Other”。

* 生效时间：用于指定执行扫描任务的时间。二维智能学习扫描任务仅执行一次。
* 复选框：（可选项）用于指定该二维扫描任务计划程序是否立即执行。

1. “勾选”表示任务部署后，达到指定时间执行二维智能学习扫描任务。若勾选此项，必须指定“任务执行”时间，否则不允许点击【确定】按钮。
2. “不勾选”表示策略部署后立即执行二维智能学习任务。

##### 编辑二维智能学习

操作步骤如下：

1. 选择“资源”>“二维智能学习”菜单。
2. 选择待编辑的记录，点击该记录最右侧操作栏内的【修改】按钮，按指定要求输入信息，点击【确定】按钮保存。

##### 删除二维智能学习

用于删除二维智能学习。操作步骤如下：

1. 选择“资源”>“二维智能学习”菜单。
2. 选择待删除的记录，点击该记录最右侧操作栏内的【删除】按钮，弹出提示窗口，点击【确定】删除。

##### 部署二维智能学习

二维智能学习任务创建完成后，需要手动部署。如果二维智能学习“未部署成功”或“已部署但未生成正反例样本库”，则在创建“规则”选择数据资源时，不能显示当前创建的二维智能学习。

##### 二维智能学习模糊查询

系统提供按“名称”、“备注”、“规则中使用”、“部署状态”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“资源”>“二维智能学习”菜单，查询条件中输入“名称”、或“备注”、或“规则中使用”、或“部署状态”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

##### 查看二维智能学习

二维智能学习资源在执行任务期间，可通过“审计” >“任务中心”任务列表查看任务执行情况。

### 发现扫描规则管理

#### 预定义发现扫描规则

通过预定义规则，可快速轻松的定义哪种类型的内容被视为敏感数据内容，预定义规则基于数据类型的检测，将预定义关键字组数据资源和预定义匹配模式数据资源作为检测目标。

预定义规则可通过派生的方式生成新的发现扫描规则。预定义发现扫描规则，数据资源间的逻辑关系缺省为“匹配任一”。

#### 预定义发现扫描规则组

系统将同类预定义规则集成到预定义规则组中，快速轻松的定义同类类型的内容被视为敏感数据内容。预定义规则组可通过派生的方式生成新的发现扫描规则组。操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”页面，在“发现扫描规则组”选项卡中，选择预定义发现扫描规则记录，点击【派生】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入发现扫描规则组名称。
* 关联业务：选择规则组所关联的“业务资源”，系统默认关联“默认业务”。
* 备注：输入规则组相关的备注信息。
* 规则：选择一个或多个预定义发现扫描规则或自定义发现扫描规则。

#### 新建发现扫描规则

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”选项卡，点击【新建】按钮，按指定要求输入各项信息，点击【确定】保存。

* 名称：输入发现扫描规则的名称，规则名称不允许有重名。
* 备注：（可选项）输入规则的备注说明。
* 敏感度：指定规则的敏感程度（很低，低，中，高，很高）。
* 【备选】列表：分类显示所有资源。资源类型分为下列几种：
* 所有：选择此项，列表将显示所有已定义的资源。
* 匹配模式：选择此项，添加匹配模式、数据识别的资源列表。
* 关键字：选择此项，添加关键字、关键字组的资源列表。
* 文档特征：选择此项，添加文档类型的资源列表。
* 文档指纹：显示文档指纹资源列表。
* 数据库指纹：显示数据库指纹资源列表。
* 智能学习：显示智能学习列表。智能学习提供要保护的数据示例。
* 数据识别资源：显示一些特定形式的数据资源,例如身份证、银行帐号、信用卡号等。
* 【修改属性】：用于设定成员列表中资源属性、阀值条件等信息，此选项仅针对关键字、关键字组生效。
* 资源名称：此处缺省显示该资源名称。
* 备注：此处缺省显示该资源备注信息。
* 条件（\*）：给规则指定数据资源，通过备选列表选择一个或多个资源到成员列表，并且定义成员列表中各资源间的逻辑关系，例如 “匹配任一”，系统将根据逻辑关系结果决定是否触发规则。
* 匹配任一：表示所有匹配条件至少满足一个，才会触发规则。

#### 编辑发现扫描规则

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”页面，选择待编辑的记录，点击【修改】按钮，按指定要求输入信息，点击【确定】按钮保存。

|  |
| --- |
| 注意：   * 策略和规则在重新编辑后，需要重新部署，否则编辑后的策略和规则不被执行。 |

#### 删除发现扫描规则

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”页面，选择待删除的记录，点击【删除】按钮，弹出提示窗口，点击【确定】删除。

#### 发现扫描规则模糊查询

系统提供按“名称”、“条件”、“备注”、“类型”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单，查询条件中输入“名称”、或“条件”、或“备注”、或“类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 新建发现扫描规则组

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”页面，在“发现扫描规则组”选项卡中，点击【新建】按钮，按指定要求输入信息，点击【确定】保存。

* 名称：输入发现扫描规则组名称。
* 关联业务：选择规则组所关联的“业务资源”，系统默认关联“默认业务”。
* 备注：输入规则组相关的备注信息。
* 关联规则：选择一个或多个预定义发现扫描规则或自定义发现扫描规则。

#### 编辑发现扫描规则组

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”页面，在“发现扫描规则组”选项卡中，选择待编辑的记录，点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除发现扫描规则组

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单。
2. 在“策略”>“发现扫描规则”页面，在“发现扫描规则组”选项卡中，选择待删除的记录，点击【删除】按钮，点击【确定】按钮保存，弹出提示窗口，点击【确定】删除。

#### 发现扫描规则组模糊查询

系统提供按“名称”、“备注”、“类型”、“启用状态”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“策略”>“发现扫描规则”菜单，在“发现扫描规则组”选项卡，查询条件中输入“名称”、或“备注”、或“类型”、或“启用状态”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 网络防护规则管理

用于设置前置过滤规则，网络传输数据优先匹配前置过滤规则，再依据策略及规则对网络中的传输数据进行匹配监控，，符合前置过滤规则的传输数据均默认放行，不对其传输数据进行内容检测（黑名单规则除外）。

此处的“黑名单”是指URL地址黑名单（需要阻止的URL地址）、发件人黑名单、收件人黑名单、文件名称黑名单（需要阻止的文件名称）。

当网络传输数据与前置过滤规则的黑名单相匹配时，将上报网络防护事件，该事件对应的规则和规则组名称为“前置规则”和“前置规则组”。

本节介绍以下内容：

* WEB代理全局设置
* WEB敏感信息过滤设置
* FTP代理全局设置
* FTP敏感信息过滤设置
* SMTP代理全局设置
* SMTP敏感信息过滤设置

#### WEB代理全局设置

操作步骤如下：

1. 选择“策略”>“网络防护规则管理”菜单，选择“WEB代理全局设置”选项卡。
2. 在“WEB代理全局设置”页面，输入相关信息，点击【提交】保存。

* 测试模式：选择此项，表示在测试模式下，当传输数据与网络防护策略、规则及前置规则黑名单匹配时，如果其动作行为是【阻止】或【重定向】，但实际动作行为仍以【审计】行为处理。
* 最大请求数：输入最大用户请求数目，不能超过1000个，0表示取默认值（默认值为1000）。
* 最大响应连接数：输入最大响应用户连接数目，不能超过1000个，0表示取默认值（默认值为1000）。
* 最大超时连接数：输入最大超时连接数目，不能超过1000个，0表示取默认值（默认值为1000）。
* 超时等待时间设置：输入超时等待时间，不能超过300秒，0表示取默认值（默认值为300）。

#### WEB敏感信息过滤设置

操作步骤如下：

1. 选择“策略”>“网络防护规则管理”菜单，选择“WEB敏感信息过滤设置”选项卡。
2. 在“WEB敏感信息过滤设置”页面，输入相关信息，点击【提交】保存。

* 添加白名单：点击【添加】按钮，输入白名单的IP地址或域名。点击【提交】保存。
* 删除白名单：选定需要删除的白名单记录，点击【删除】按钮进行删除。
* 添加黑名单：点击【添加】按钮，输入黑名单的IP地址或域名，点击【提交】保存。

删除黑名单：选定需要删除的黑名单记录，点击【删除】按钮进行删除。

* 请求设置
* 请求类型：包括Get、Head、Options、Post、Put、Delete、Trace、connect八种。

Get：从设备读取数据，这些数据通常是操作参数，例如连接状态、接口名称等；

Head：标签用于定义网页文档的头部，其中的 中的元素可以引用脚本、指示浏览器在哪里找到样式表、提供元信息等等；

Option：定义下拉列表中的一个选项（一个条目）；

Post：用来向目的服务器发出更新请求，并附有请求实体；

Put：用来更新资源；

Delete：通过http请求删除制定的URL上的资源；

Trace：用来调用一个远程的请求信息应用程序层的循环后退。

Connect：转换为透明TCP/IP隧道的连接请求。

* 请求体积上限：表示“数据体积大于指定值时该请求自动忽略，放行处理”，输入请求体积上限值，单位KB，取值范围为1至100000的整数。
* 请求体积下限：表示“数据体积小于指定值时该请求自动忽略，放行处理”，输入请求体积下限值，单位KB，取值范围为1至100000的整数。
* 终端代理：当“指定特定终端代理发送的数据不进行过滤”时设置此项。点击右边按钮，选择终端代理类型,点击“选择”即可。
* MIME类型：当“指定MIME类型的数据不进行过滤”时设置此项。点击右边按钮，选择MIME类型，点击“选择”即可。
* 响应设置
* 忽略小于指定大小的响应：输入忽略小于指定大小的响应值，单位KB，表示“数据体积小于设置值时该响应自动忽略，放行处理”，取值范围为1至100000的整数。
* 文件设置
* 忽略没有文件的请求/响应：点击此项，表示忽略没有文件的请求/响应。

文件大小：当包含文件的请求/响应中，文件体积大小超过指定值，所有文件被过滤，放行处理。输入文件体积数值，单位KB，取值范围为0至100000的整数。

文件数量：当包含文件的请求/响应中，文件数量超过指定值，则超出数量的文件附件被过滤，放行处理，在数值范围内的附件仍被检测。输入文件数量，单位个，取值范围为1至32的整数。

文件名称：当“监控到指定文件名称的文件在网络环境中传输时”该文件被自动阻止（文件名称黑名单）。在文件名称列表中选择需要被阻止的文件名称记录即可。

#### FTP代理全局设置

操作步骤如下：

1. 选择“策略”>“网络防护规则管理”菜单，选择“FTP代理全局设置”选项卡。
2. 在“FTP代理全局设置”页面，输入相关信息，点击【提交】保存。

* 测试模式：选择此项，表示在测试模式下，即使传输数据与网络防护策略、规则及前置规则匹配时，如果动作行为是【阻止】或【隔离】，但动作行为仍以【审计】行为处理。
* 连接超时时间：输入链接超时时间，时间不能超过300秒， 0表示取默认值（默认值为300）。
* 最大连接数：输入最大用户连接数目，不能超过1000个，0表示取默认值（默认值为1000）。
* 启用隔离服务器：勾选此项，表示隔离服务器已启用，制定FTP策略时，动作可选择【隔离】。（此处的隔离服务器指ftp服务器）。

服务器地址：输入ftp服务器的IP地址或域名。

账号：输入隔离服务器的账号名（即ftp服务器中创建的用户名）。

密码：输入隔离服务器的账号对应的密码（即ftp服务器用户名对应的密码）。

测试链接：输入IP地址及用户名、密码后可点击【测试链接】按钮验证输入的认证信息是否有效，如果显示链接成功，则说明认证信息正确有效。

#### FTP敏感信息过滤设置

操作步骤如下：

1. 选择“策略”>“网络防护规则管理”菜单，选择“FTP敏感信息过滤设置”选项卡。
2. 在“FTP敏感信息过滤设置”页面，输入相关信息，点击【提交】保存。

* FTP命令：包含put、get两种。

Get：当监控“从FTP服务器下载或读取的数据”时，勾选此项。

Put：当监控“向FTP服务器上传的数据”时，勾选此项。

* 文件大小：当通过ftp服务器上传或下载文件的体积超过指定值，则该文件附件被过滤，自动放行。输入文件体积数值，单位KB，取值范围为0至64000的整数。
* 文件名称：输入需要阻止的文件名称。

#### SMTP代理全局设置

操作步骤如下：

1. 选择“策略”>“网络防护规则管理”菜单，选择“SMTP代理全局设置”选项卡。
2. 在“SMTP代理全局设置”页面，输入相关信息，点击【提交】保存。

代理参数设置：

* 测试模式：选择此项，表示在测试模式下，即使传输数据与网络防护策略、规则及前置规则匹配时，如果动作行为是【阻止】或【转发至管理员】或【添加邮件标头】，但动作行为仍以【审计】行为处理。
* 连接超时时间：输入连接超时时间，不能超过300秒，0表示取默认值（默认值300）。
* 最大接收者数：表示最大接受者数不能超过指定值，接受者数量超过指定值的邮件自动被阻止发送。输入最大接收者数目，不能超过256个。
* 最大连接数：输入最大连接数目，不能超过1000个。
* 最大数据量：表示最大数据量不能超过指定值，数据量超过指定值的邮件自动被阻止发送。输入最大数据量，不能超过64M。

邮件服务器设置：

* 邮件服务器IP：输入邮件服务器IP地址。
* 域名：输入邮件服务器的域名。

转发邮件服务器设置：

* 是否转发邮件：勾选此项，表示转发邮件已启用。
* 转发邮件服务器地址：输入SMTP邮件服务器IP地址或域名。
* 转发邮件服务器端口域名：输入转发邮件服务器的端口（邮箱服务器端口范围：0~65535）。
* 管理员邮箱：输入管理员邮箱的地址。
* 邮箱密码：输入邮箱密码。
* 测试链接： IP地址以及用户名、密码输入完成后可点击【测试链接】按钮查看该认证信息与IP地址是否匹配，如果显示链接成功，则说明认证信息正确。

#### SMTP敏感信息过滤设置

操作步骤如下：

1. 选择“策略”>“网络防护规则管理”菜单，选择“SMTP敏感信息过滤设置”选项卡。
2. 在“SMTP敏感信息过滤设置”页面，输入相关信息，点击【提交】保存。

* 文件大小：表示文件体积超出此数值被过滤，自动放行。输入文件大小，单位“KB”，取值范围为0至64000的整数。
* 文件数量:表示文件数量超出此数值的文件被过滤，自动放行，在此数值范围内的文件仍进行检测防护。输入文件数量，单位“个”，取值范围为1至32的整数。
* 文件名称：输入需要阻止的文件名称。
* 发件人白名单

添加白名单：点击【添加】按钮，输入发件人白名单邮件地址，点击【提交】按钮保存。

删除白名单：选定需要删除的发件人白名单记录，点击【删除】按钮进行删除。

* 发件人黑名单

添加黑名单：点击【添加】按钮，输入发件人黑名单邮件地址，点击【提交】保存。

删除黑名单：选定需要删除的发件人黑名单记录，点击【删除】按钮进行删除。

* 收件人白名单

添加白名单：点击【添加】按钮，输入收件人白名单邮件地址，点击【提交】保存。

删除白名单：选定需要删除的收件人白名单记录，点击【删除】按钮进行删除。

* 收件人黑名单

添加黑名单：点击【添加】按钮，输入收件人黑名单邮件地址，点击【提交】保存。

删除黑名单：选定需要删除的收件人黑名单记录，点击【删除】按钮进行删除。

### 网络防护策略管理

系统针对不同网络防护规则，提供不同的网络防护策略类型，发现策略包含以下几种类型：

* WEB策略
* FTP策略
* SMTP策略

#### 新建WEB策略

操作步骤如下：

1. 选择“策略”>“网络防护策略”菜单。
2. 在“策略”>“网络防护策略”页面，点击【添加策略】按钮，选择【添加WEB策略】选项，按指定要求依次输入信息，点击【确定】保存。

* 名称：输入策略的名称。
* 描述：输入关于当前新建WEB策略的描述说明。
* 源IP地址：将备选的源IP地址添加到列表中。
* 目的IP地址：将备选的目的IP地址添加到列表中。
* 关联规则组：将备选的关联规则组添加到列表中。

请求响应连接设置：

* URL设置：仅“检测指定URL地址”时设置此项。输入URL地址后，点击【添加】按钮即可。
* 文件设置：仅“检测指定文件名称的文件或邮件附件”时设置此项，将备选的附件名称添加到列表中。“文件名称”数据资源可通过“首页>资源>文档特征”模块进行管理。
* 动作设置：当敏感信息在被监控网络环境中违规传输时采取的防护响应。包括审计、阻止和重定向三种。
* 审计：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时上报审计事件。
* 阻止：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时将对此数据传输行为进行阻止。
* 重定向：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时，访问链接页面会重新定向到一个自定义页面，选择此选项时，需要指定“重定向URL地址”。

#### 新建FTP策略

操作步骤如下：

1. 选择“策略”>“网络防护策略”菜单。
2. 在“策略”>“网络防护策略”页面，点击【添加策略】按钮，选择【添加FTP策略】选项，按指定要求依次输入信息，点击【确定】保存。

* 策略名称：输入策略的名称。
* 描述：输入关于当前新建策略的描述说明。
* 源IP地址：将备选的源IP地址添加到列表中。
* 目的IP地址：将备选的目的IP地址添加到列表中。
* 关联规则组：将备选的关联规则组添加到列表中。

FTP高级设置：

* FTP用户设置：仅“检测指定FTP用户”时设置此项。可以通过“添加”按钮输入指定FTP用户名即可。
* 文件设置：仅“检测指定文件名称的文件”时设置此项，将备选的文件名称添加到列表中。“文件名称”数据资源可通过“首页>资源>文档特征”模块进行管理。
* 动作设置：当敏感信息在被监控网络环境中违规传输时采取的防护响应。包括审计、阻止和隔离三种。
* 审计：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时上报审计事件。
* 阻止：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时将对此数据传输行为进行阻止。
* 隔离：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时将对此敏感数据文件进行隔离。选择【隔离】响应时，应“启用隔离服务器”并设置可到达服务器地址的有效认证信息，否则敏感数据文件将不能被正确隔离至指定目标目录。

#### 新建SMTP策略

操作步骤如下：

1. 选择“策略”>“网络防护策略”菜单。
2. 在“策略”>“网络防护策略”页面，点击【添加策略】按钮，选择【添加SMTP策略】选项，按指定要求依次输入信息，点击【确定】保存。

* 策略名称：输入策略的名称。
* 描述：输入关于当前新建策略的描述说明。
* 源IP地址：将备选的源IP地址添加到列表中。
* 目的IP地址：将备选的目的IP地址添加到列表中。
* 关联规则组：将备选的关联规则组添加到列表中。

邮件发送设置：

* 邮件设置：仅“检测指定邮箱地址”时设置此项。可分别设置指定的“发件人邮箱地址”、“收件人邮箱地址”。分别输入收件人、发件人的邮箱地址，点击【添加】按钮进行添加，点击【删除】按钮进行删除即可。
* 文件设置：仅“检测指定文件名称的文件”时设置此项，将备选的文件名称添加到文件列表中。“文件名称”数据资源可通过“首页>资源>文档特征”模块进行管理。
* 动作设置：包括添加邮件标头、阻止、转发到管理员、审计四种。

添加邮件标头：表示将违反策略的邮件自动添加一个标头进行发送，相当于一个标识，告知用户这个邮件存在敏感数据泄漏风险。

阻止：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时将对此邮件发送行为进行阻止。

转发到管理员：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时，将匹配到的敏感信息邮件转发至指定管理员邮箱。

审计：表示依照策略及规则对网络中的传输数据进行匹配监控，监控到敏感信息在网络环境中违规传输时上报审计事件。

#### 删除网络防护策略

用于删除网络防护信息。操作步骤如下：

1. 选择“策略”>“网络防护策略”菜单。
2. 在“策略”>“网络防护策略”页面，选择待删除的记录，点击【🗑删除】按，钮弹出提示窗口，点击【确定】删除。

#### 网络防护策略模糊查询

系统提供按“名称”、“策略类型”、“描述”、“状态”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“策略”>“网络防护策略”菜单，查询条件中输入“名称”、或“策略类型”、或“描述”、或“状态”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 网络防护事件管理

用于查看和维护“网络防护策略”生成的发现事件及详细信息。

工具栏包括以下功能：

* 查看事件详细信息。
* 管理事件工作流。
* 上报事件。
* 其他功能：查询、刷新、显示列管理。

#### 查看事件详细信息

默认情况下，事件列表按其检测时间降序排序，也可以单击表格中任意列标题上的▼或▲箭头将它们排序（升序或降序）。

查看事件详细信息，可选中事件，点击事件列表下方的【详细信息】选项卡即可显示事件详细内容，如时间、策略名称、数据、状态、敏感度、规则组名称、组织名称、规则名称、标签、业务名称、匹配内容、状态、客户端、服务IP、客户端IP等。

查看事件审核记录，可选中事件，点击事件列表下方的【审核记录】选项卡即可显示该时间相关的历史操作记录。

#### 查询网络防护事件

可对事件进行单条件查询、组合条件查询。查询事件操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，点击【事件查询】title可显示查询条件信息。
3. 需根据更多条件查询事件，点击【更多】按钮，系统显示全部查询条件。
4. 输入查询条件，点击【查询】按钮即可。

查询条件的内容属性如下：

* + 敏感度：根据敏感度查询事件。
  + 业务名称：根据业务名称查询事件。
  + 组织名称：根据组织名称查询事件。
  + 策略名称：根据触发事件的策略名称查询事件。
  + 规则名称：根据触发事件的规则名称查询事件。
  + 时间：根据触发事件的时间查询事件。
  + 规则组：根据规则组名称查询事件。
  + 客户端：根据事件的客户端IP查询事件。
  + 服务端：根据触发事件的服务端IP查询事件。
  + 匹配内容：根据匹配内容查询事件。
  + 状态：根据事件状态查询事件。
  + 每日时间：根据每天触发事件时的起始时间和结束时间查询事件。

#### 管理事件工作流

用于管理所选事件的工作流。

本节描述以下内容：

* 改变状态
* 改变敏感度
* 忽略事件

##### 改变状态

用于更改事件状态、管理维护事件状态标签。

* 更改状态：更改事件状态。系统提供三项预定义状态：新建、处理、关闭，以上三种状态不允许编辑、删除。

操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，勾选任意事件（可多选），点击【工作流】下拉菜单，选择【改变状态】子菜单，选择需要更改的状态选项，例如选择【关闭】状态。
3. 双击该事件记录，在事件列表的【审核记录】选项卡中，更新显示已更改状态记录。

* 管理状态：用于管理自定义事件状态。可进行新建、删除、调整显示顺序操作。
* 新建【状态】：用于添加新的事件状态。操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，点击【工作流】下拉菜单，选择【改变状态】子菜单，再选择【管理状态】选项。
3. 在“事件状态管理”页面，点击【新建】按钮。
4. 在“状态属性”页面，按指定要求输入信息，点击【确定】按钮保存。

名称：（\*）用于输入状态名称（不允许重名，且少于32个字符。）

描述：（可选项）为事件状态添加备注。

图标：用于为事件状态选择旗标。

* 删除【状态】：用于删除自定义事件状态。操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，点击【工作流】下拉菜单，选择【改变状态】子菜单，再选择【管理状态】选项。
3. 在“事件状态管理”页面，勾选一条或多条自定义状态记录，点击【删除】按钮。
4. 在“确定要删除已选择的状态吗?”提示窗口，点击【确定】按钮确认删除。

* 调整显示顺序：调整状态的显示顺序。通过选择一个状态单击向上或向下箭头来选择状态的排列顺序。按状态排序，排序结果将会反应在报表和事件列表中。操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，点击【工作流】下拉菜单，选择【改变状态】子菜单，再选择【管理状态】选项。
3. 在“事件管理状态”页面，勾选一条事件状态记录，点击▲或▼按钮完成排序显示。

##### 改变敏感度

用于更改事件的敏感度级别，即改变事件的敏感度（包括很高、高、中等、低、很低五个等级），是衡量该事件对系统影响程度的重要标准。事件敏感度在创建网络防护规则时指定，系统默认级别为“很低”。

操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“审计”>“网络防护事件”页面，勾选任意事件（可多选），点击【工作流】下拉菜单，选择【改变敏感度】子菜单，再选择需要更改的敏感度级别。
3. 双击该事件记录，在事件列表的【审核记录】选项卡中，显示更改记录。

##### 忽略事件

表示将事件标记为“忽略”或“取消标记已忽略”的事件。

* 忽略：选择此项，表示如果已审查事件并且不采取任何操作，请将事件标记为忽略。

操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“审计”>“网络防护事件”页面，勾选任意事件（可多选），点击【工作流】下拉菜单，选择【忽略事件】子菜单，在选择【忽略】选项。
3. 双击该事件记录，在事件列表的【审核记录】选项卡中，显示更改记录。

##### 上报事件

将所选事件通过电子邮件上报给相关管理人员，或上报给其他人员。

操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，选择任意事件（可多选），点击【上报】按钮。
3. 在“发送事件”界面中，按指定要求输入信息，点击【确定】保存。

* 收件人：（\*）输入收件人电子邮箱地址。
* 抄送、密送：（可选）若想将副本或无信头副本发送到其他人员，可输入抄送和密送人员的邮箱地址。
* 主题：（\*）输入邮件的主题信息。主题下方文本框显示上报操作执行时间，所选事件的扫描方式、敏感度等级、事件ID等信息。

##### 其他功能

用于刷新事件。详细描述如下：

* 【刷新】按钮：用于刷新当前界面信息。

操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，点击按钮即可。

* 显示列管理：用于管理事件列表的显示列，可设置列的显示顺序、列宽等信息。

操作步骤如下：

1. 选择“审计”>“网络防护事件”菜单。
2. 在“首页”>“审计”>“网络防护事件”页面，点击【显示列表管理】按钮，进入弹出的显示列管理页面。
3. 点击▼或▲箭头以调整显示顺序，双击要更改的列，输入列宽度。
4. 双击需要修改的列信息，更改列描述信息（最多输入255个字符）。
5. 勾选需要被显示的列，最多显示7列。
6. 点击【确定】按钮。

### 全局状态设置

用于设定状态模块全局视图显示的报表。设置完成后，在“状态”界面可显示设定的内容。系统以“饼图形式”显示不同类型的统计报表。系统支持报表类型的统计方式：网络防护。

操作步骤如下：

1. 选择“审计”>“全局状态设置”菜单。
2. 点击“统计类型”列表下拉控件，选择要在“状态”界面显示的网络防护报表。
3. 选择图表类型。
4. 选择图表显示位置。
5. 选择要显示的报表内容。
6. 点击【保存】按钮。

|  |
| --- |
| 提示：   * 若需查看某柱体总览信息，将鼠标放至该柱体上方即可，系统以悬浮窗形式显示其总览信息。 * “统计类型”选择“网络防护”时，报表内容显示网络防护报表相关信息。 |

### 报表计划任务

用于查看和维护事件报表的计划任务。

计划任务是在指定时间将事件报表以邮件形式发送到用户的邮箱，方便用户及时了解已发现的敏感内容的统计结果。

报表计划任务列表显示以下内容：

* 任务名称：报表计划任务名称。
* 执行周期：任务是以何种周期执行，分为天、周、月三种方式。
* 开始运行时间：报表计划任务的开始执行时间。
* 结束运行时间：报表计划任务的结束执行时间。
* 所有者：报表计划任务的创建者。
* 状态：报表计划任务的当前状态，有启用、停用两选项。
* 备注：报表计划任务的备注信息。
* 操作：对报表计划任务可执行的操作，系统提供两种操作方式：修改、删除。

本节描述以下内容：

* 新建报表计划任务
* 编辑报表计划任务
* 删除报表计划任务

#### 新建报表计划任务

用于添加新的报表计划任务。

操作步骤如下：

1. 选择“审计”>“报表计划任务”菜单，点击【新建】按钮。
2. 在“首页”>“审计”>“报表计划任务”>“新建计划任务”页面，按指定要求依次输入信息，点击【确定】保存。

页面内容如下所示：

* 基本设置：用于指定计划任务存储的位置和针对哪些内容进行任务调度。
* 任务名称：输入您要报表计划的任务的名称。
* 备注：（可选）输入该报表计划的可描述信息。
* 报表分类：指定监控报表所从属的报表分类。
* 报表类别：指定发送报表所从属的报表类别。
* 报表名称：指定需要发送的报表，可从下拉列表选择。报表名称列表内容与报表类别关联，仅显示选定的报表类别下的报表内容。
* 计划：设置任务的开始时间、结束时间和执行周期。
* 计划开始：设定报表计划的开始时间。
* 计划周期：设定报表计划的执行周期。与【选项】配合使用。

1. 天：选择此项，表示任务在每天的相同时间执行，并在【选项】中输入每天定时执行任务的时间。
2. 周：选择此项，表示任务在每周的指定时间（1:30）循环执行。系统默认每周一凌晨执行计划任务。如需设置自定义时间，可在【选项】中勾选每周定时执行的时间。
3. 月：选择此项，表示任务在每个月的指定日期循环执行。此项无系统默认值，需用户设置在【选项】模块输入每月任务执行的时间。当输入多个日期时，请使用英文格式的逗号“,”间隔。

|  |
| --- |
| 注意：  计划周期选择每天：默认为凌晨发送邮件，若设置时间则在指定时间发送邮件；每周：指定时间的每晚1：30发送邮件；每月：指定时间的每晚3点发送邮件。 |

1. 截止日期：设定报表计划任务的截止日期。
2. 状态设置：设定任务执行情况。选择“启用”时，计划任务按设定的信息发送内容；选择“停用”时，计划任务不发送任何内容。

* 邮件设置：用于指定报表发送的主题、收件人。
* 收件人：指定报表邮件的收件人。

点击【修改】按钮，在“选择收件人”页面的可选用户列表中，勾选要发送邮件通知的用户，点击“▶”按钮，再点击【提交】按钮。

* 抄送地址：指定邮件的抄送人员。输入多个抄送人员邮箱地址时，使用逗点将其隔开。

#### 编辑计划任务

用于修改报表任务计划。

操作步骤如下：

1. 选择“审计”>“报表计划任务”菜单。
2. 在“首页”>“审计”>“报表计划任务”页面，选择要编辑的记录，点击【修改】按钮，按指定要求依次输入信息，点击【确定】保存。

#### 删除计划任务

用于删除报表任务计划。

操作步骤如下：

1. 选择“审计”>“报表计划任务”菜单。
2. 在“首页”>“审计”>“报表计划任务”页面，选择要删除的记录，点击【删除】按钮，系统弹出提示窗口，点击【确定】按钮删除。

#### 报表计划任务模糊查询

系统提供按“名称”、“所有者”、“备注”、“状态”、“开始运行时间”、“结束运行时间”模糊查询功能，支持组合查询。

操作步骤如下：

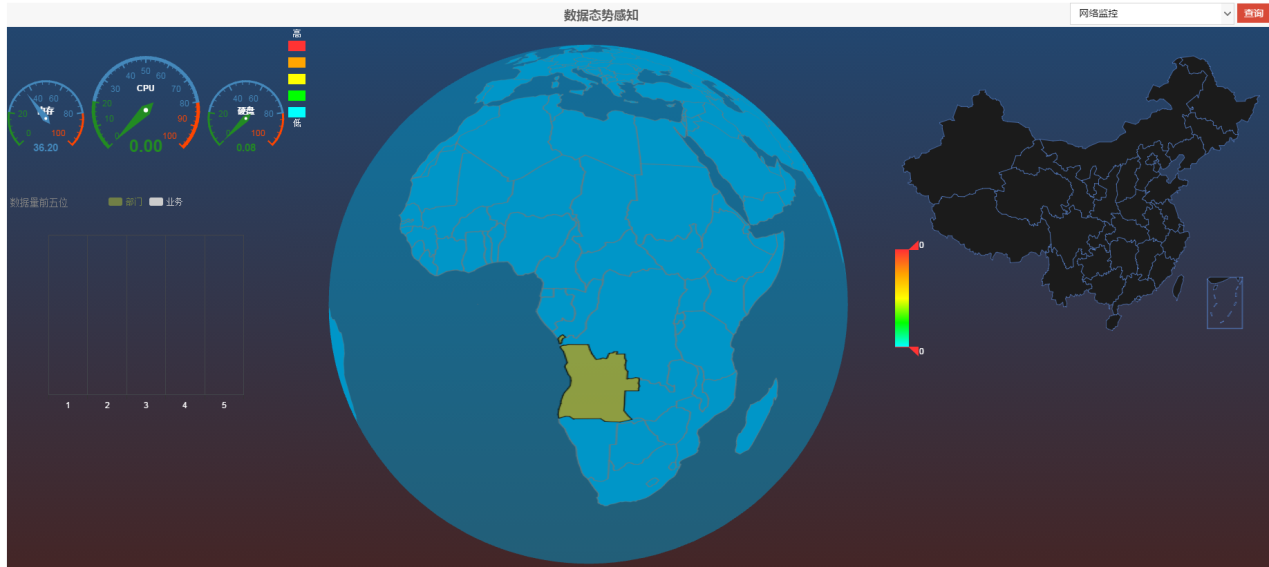
1. 选择“审计”>“报表计划任务”菜单，查询条件中输入“名称”、“所有者”、“备注”、“状态”、“开始运行时间”、“结束运行时间”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 报表计划任务列表排序

系统默认以报表计划任务创建时间的先后顺序显示，当需要对任务列表内容进行排序时，点击要排序列内容的列表头即可。

### 全球数据态势感知

全球数据态势感知动态展现企业敏感数据的网络流向、按安全事件敏感度统计、按部门及业务统计敏感数据数量、按传输协议统计传输敏感数据。如下图所示：



1. 系统信息仪表盘：显示SIMP-DPS系统中当前内存、CPU、存储磁盘的使用情况。
2. 安全态势:通过分析网络防护事件了解敏感数据的流向及风险预测。
3. 统计事件：以柱状图形式显示“网络防护事件数量排名前五位的业务资源”。
4. 事件统计：以玫瑰饼图形式显示“网络防护事件数量中排名前八位的传输协议”。
5. 中国地区态势图：数据传输中国区态势图。
6. 全球3D态势图：全球数据传输3D态势图。

### 报表风格设置

用于设置系统产生的报表样式。如需自定义报表风格，可根据需要设置“报表封面图片”、“报表背景水印图片”、“企业logo”的任意一种或多种。

操作步骤如下：

1. 选择“审计”>“报表风格设置”菜单。
2. 在“首页”>“审计”>“报表风格设置”页面，点击“报表封面图片”的【浏览】按钮，选择要上传的图片，点击【打开】按钮，点击【上传】按钮。
3. 点击“报表背景水印图片”的【浏览】按钮，选择要上传的图片，点击【打开】按钮，点击【上传】按钮。
4. 点击“企业logo”的【浏览】按钮，选择要上传的图片，点击【打开】按钮，点击【上传】按钮。

|  |
| --- |
| 注意：   * 上传的文件必须图片格式，且必须是 jpg, jpeg 或 png格式。 * 报表封面图片上传的图片文件大小必须为768 × 1024。 * 报表背景水印图片上传的图片文件大小必须为768 × 1024。 |

### 网络防护报表

用于设定和维护“网络防护策略”事件统计报表。可以新建报表、另存报表、删除报表、新建报表分类。

#### 报表分类管理

本节描述报表分类新建、修改、删除操作。

##### 新建报表分类

用于新建报表分类。

操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”>“审计”>“网络防护报表”页面，点击按钮。
3. 在“报表分类”页面，按指定要求依次输入信息，点击【确定】保存。

* 分类名称：（\*）输入报表的分类名称（分类名称不允许重复，最多输入128个字符）。
* 备注：输入报表分类的描述信息。

##### 编辑报表分类

操作步骤如下：

1. 进入“首页”>“审计”>“网络防护报表”页面，选择要修改的报表分类，点击按钮。
2. 在“报表分类”页面，输入报表分类名称和备注信息。

##### 删除报表分类

报表分类中”默认报表分类”类别不可删除。系统提供两种删除报表分类的方法：在“报表分类”下拉列表中删除，或在“已有报表”列表中删除。

方法一，在“报表分类”下拉列表中删除的操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”>“审计”>“网络防护报表”页面，报表属性中点击【报表分类】下拉列表，选择要删除的报表分类，点击按钮，弹出提示窗口，点击【确定】删除。

方法二，在“已有报表”列表中删除的操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”>“审计”>“网络防护报表”页面，已有报表中选择要删除的报表分类，点击按钮。

|  |
| --- |
| 注意：   * 若删除的报表分类下存在报表，则这些报表将被存储在“默认分类”报表分类下。 |

#### 报表管理

本节描述报表新建、修改、删除操作。

##### 新建报表

系统提供两种新建报表操作方式：“保存”报表和“另存为”报表。

##### 保存报表

操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”>“审计”>“网络防护报表”页面，选择所从属的报表类别、报表分类信息（可选）。
3. 选择要查询的报表条件（可选）。
4. 点击【保存】按钮，输入报表名称和报表描述（\*），点击【确定】按钮。

##### 报表另存为

方便用户在已有报表基础上派生新的报表。

操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”>“审计”>“网络防护报表”页面，选择另存为的报表原型，如点击“网络防护报表”>默认报表分类>“*网络防护事件明细*”。
3. 编辑新报表的查询条件，点击【另存为】按钮。输入“报表名称”，点击【确定】按钮保存。

##### 删除报表

用于删除系统的非预定义报表。

操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”> “审计”>“网络防护报表”页面，已有报表中选择要删除的非默认报表，点击按钮，弹出提示窗口，点击【确定】删除。

##### 查询报表

用于查询报表内容。可对报表进行单条件查询、组合条件查询。系统默认以组织资源统计发现事件信息，结果以柱形图或折线图形式显示。

查询报表操作步骤如下：

1. 选择“审计”>“网络防护报表”菜单。
2. 在“首页”>“审计”>“网络防护报表”页面，分别在报表属性、常规条件、其他条件中选择或输入查询条件，点击【查询】按钮。
3. 如需查看查询结果各统计依据的总览信息，可将鼠标放至该统计依据柱体上方，系统将以浮窗形式显示总览数据。
4. 如需查看查询结果各统计依据的详细信息，点击该统计依据柱形即可，系统将在图表下方以列表形式显示详细内容。

查询条件的内容属性如下：

* + 报表属性：
* 报表类别：查询“网络防护策略”下的报表内容。
* 统计方式：查询结果中X轴显示内容，有“按组织资源统计”、“按业务资源统计”、“按时间统计”三种显示方式。

1. 按组织资源统计：统计由组织资源关联的策略生成的事件总数。
2. 按业务资源统计：根据由业务资源关联的策略生成的事件总数。
3. 按时间统计：根据时间统计文件总数。选择此项时，“时间粒度”选项可用，否则，“时间粒度”选项不可用。

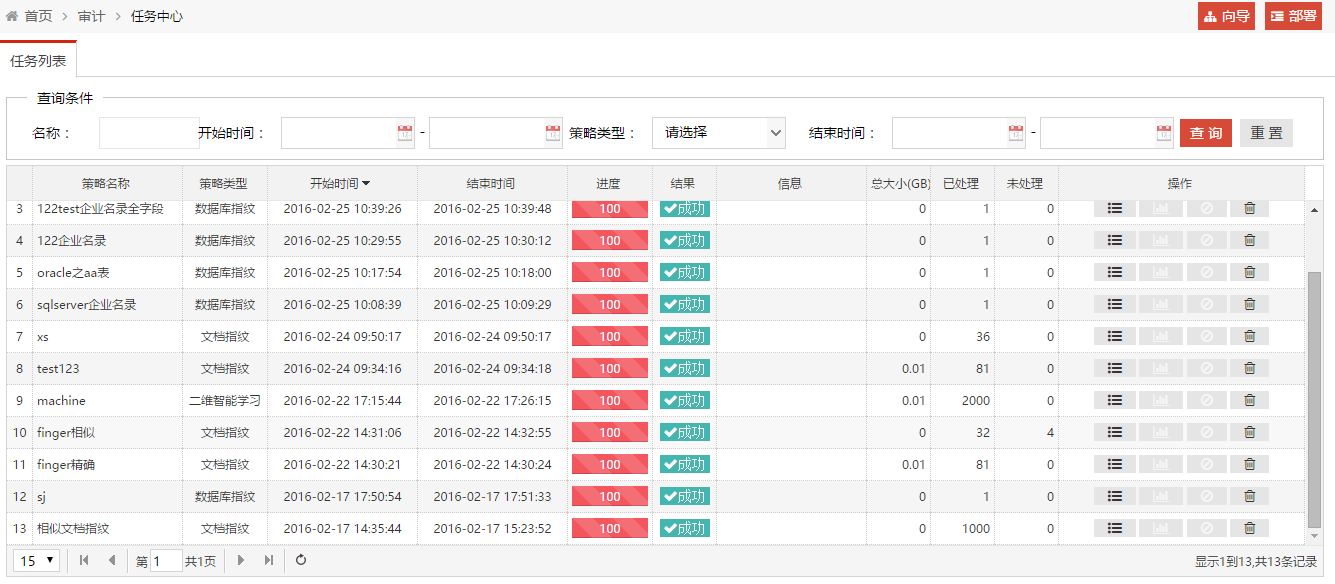
* 报表分类：选择指定报表分类后，新保存或另存为的报表存储至所选的报表分类下。
* 报表类型：显示报表的显示类型，系统预置形式显示。
* 统计依据：指定统计报表时显示的分组方式。
* TOP N：显示网络防护策略触发事件总数最多的前N项内容，只可输入1-12之间的数字。
* 排序：将各统计依据的各维度值的事件总数以正序（从小到大）或反序（从大到小）排列。
* 时间粒度：统计所选时间内的事件总数。系统默认统计“最近一季度”，且默认不可更改。当统计方式选择“按时间统计”时，此选项显示为可用。系统提供四种时间维度：“最近一季度”、“最近一月”、“最近一周”、“最近24小时”。
  + 常规条件：
* 组织资源类型： 当统计方式选择“组织资源统计”或“业务资源统计”时，统计所选择组织资源触发事件的总数。当统计方式为“按业务统计”并且统计依据为“业务类型”时，此处的常规条件中“组织资源类型”禁用。
* 业务类型：当统计方式选择“组织资源统计”或“业务统计”时，统计所选择业务资源触发事件的总数。当统计方式为“按组织资源统计”并且统计依据为“组织资源类型”时，此处的常规条件中“业务类型”禁用。
* 客户端IP：根据触发事件的客户端IP地址查询报表。
* 服务IP：根据触发事件的服务IP地址查询报表。
* 敏感度：统计网络防护策略中所选择敏感度。
  + 其他条件：
* 防护策略：根据防护策略查询生成事件的报表。
* 规则组：根据规则组名称查询生成事件的报表。
* 规则：根据规则名称查询生成事件的报表。
* 状态：根据事件状态查询报表。
* 标题：根据触发事件的标题查询报表。
* 附件名：根据触发事件的附件名查询报表。
* 发件人：根据触发事件的收件人查询报表。
* 收件人：根据触发事件的发件人查询报表。
* 附件大小：根据触发事件的文件大小查询报表，文件大小以KB为单位。
* 检测日期：根据触发事件的检测日期查询报表。
* 每日时段：根据触发事件的时段查询报表。

|  |
| --- |
| 注意：   * 不输入查询条件时，系统默认查询“网络防护”报表的“默认分类”类别下数量最多的前5项（TOP5）“组织资源”内容。 * 报表属性的统计方式选择“按组织资源统计”，统计依据若不选择“业务类型”，则常规条件的“组织资源类型”不可选择。 * 报表属性的统计方式选择“按业务统计”，统计依据若不选择“组织资源类型”，则常规条件的“业务类型”不可勾选。 * 报表的详细内容列表支持排序和翻页功能。 |

### 任务中心

用于管理和维护系统下发的任务。可对任务中心的高级资源 “任务”进行删除、查看任务的详细信息等操作。

此模块仅显示部署成功的高级资源“任务”，未部署的“任务”不显示。



任务列表中内容解释如下：

* 策略名称：“高级资源”名称。
* 策略类型：任务的所属类型。系统提供3类不同的任务类型：“文档指纹”、“数据库指纹”、“二维智能学习”。
* 开始时间：执行高级资源的开始时间。
* 结束时间：执行高级资源的结束时间
* 执行进度：任务执行的进度，即任务已分析文件体积占扫描目标文件总体积的比率。
* 执行结果：任务的执行结果。系统存在以下几种执行结果：部署成功、启动中、运行中、停止中、停止、成功、失败、完成（高级资源任务中根据业务要求禁止停止、启动任务）。
* 已部署：高级资源任务或策略部署后置为“部署成功”状态。
* 运行中：高级资源任务或策略正在执行。
* 停止中：高级资源任务或策略由“启动”状态变为“停止”状态的中间过程。
* 停止：任务点击“停止”后的最终状态。
* 成功：高级资源任务或策略完成文件扫描，且文件分析完成。
* 失败：高级资源任务或扫描策略未发现目标文件，导致任务执行失败。任务执行失败可能由于网络、认证信息输入错误等原因导致。
* 完成：策略发现目标文件但部分文件处理失败，处理失败包含解析文件内容错误、获取文件内容错误、扫描数据表发生错误等原因。
* 信息：显示处理文件失败的原因。
* 总大小：已扫描文件的总体积（单位G），当扫描数据的体积小于50M，此处显示为0G（忽略不计）。
* 已处理：已处理的文件总数。
* 未处理：未处理的文件总数。
* 操作：任务可执行的操作内容。包含以下五种操作：

| 图标 | 操作名称 | 操作描述 |
| --- | --- | --- |
|  | 查看详细 | 查看该任务执行的详细情况。 |
|  | 启动 | 启动任务。 |
|  | 停止 | 暂停任务。运行中的高级资源任务停止按钮不可用。 |
|  | 删除 | 删除任务执行记录（含全部历史执行记录）。 |

#### 任务中心模糊查询

系统提供按“名称”、“开始时间”、“策略类型”、“结束时间”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“审计”>“任务中心”菜单，查询条件中输入“名称”、“开始时间”、“结束时间”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

#### 查看详细

查看高级资源任务历次执行情况，包括任务类型、开始时间、结束时间、运行结果、已处理、未处理文件个数等。出现在任务列表中的任务均可执行此操作。操作步骤如下：

1. 选择“审计”>“任务中心”菜单。
2. 进入到“首页”>“审计”>“任务中心”页面，选择要查看的策略任务。
3. 点击图标，切换至“任务详细信息”选项卡，列表显示任务执行的历史记录。单击某条历史记录，显示该记录的“已处理文件列表”、“未处理文件列表”。“已处理文件”列表显示分析成功文件的所属路径、扫描时间，“未处理文件”列表显示分析失败文件的路径及失败原因。

#### 启动任务

启动高级资源任务。

操作步骤如下：

1. 选择“审计”>“任务中心”菜单。
2. 进入到“首页”>“审计”>“任务中心”页面，选择要启动的任务。
3. 点击图标。任务立刻执行。未执行完成的任务继续执行，已执行完成的任务立即执行差异扫描。

启动后的任务，其执行进度、已处理文件、未处理文件均根据执行情况实时更新，直至任务执行完成。任务执行完成后的状态最终可显示为“成功”或“完成”。

|  |
| --- |
| 提示：  高级资源任务状态为 “运行中”时，【停止】图标不可操作。  高级资源被规则引用后，【启动】图标不可操作。 |

#### 停止任务

在高级资源任务中，无【停止】按钮。运行中的高级资源任务，不允许点击【停止】按钮。

#### 删除任务执行记录

用于删除任务中心显示的记录。该操作仅删除任务中心的执行记录，不会删除策略模块和高级资源模块的记录。

当任务中心的状态为“运行中”、“停止中”时，删除图标不可操作。

操作步骤如下：

1. 选择“审计”>“任务中心”菜单。
2. 进入到“首页”>“审计”>“任务中心”界面，选择要删除的策略记录。
3. 点击图标，系统弹出的“确定要删除该任务吗” 提示窗口，点击【确定】删除。

|  |
| --- |
| 提示：  “任务中心”页面的【删除】功能仅删除列表中的记录，并非删除高级资源任务，如果要删除高级资源，请进入“高级资源”模块列表执行删除操作。 |

### 个人中心

#### 查看用户信息

选择“系统”>“个人中心”菜单，显示当前登录用户的详细信息，包括用户名、电子邮箱地址、当前用户的所属角色。

#### 向导设置

* 自动显示向导：指用户首次登录系统时，系统自动弹出“向导帮助”页面，引导用户使用系统。
* 手动显示向导：指用户首次登录系统时，系统不弹出“向导帮助”页面，如需要使用向导功能，需点击系统页面右上角的【向导】按钮，来进入“向导帮助”页面。

#### 更改密码

修改当前登录用户的密码。操作步骤如下：

1. 点击“系统”>“个人中心”菜单，将打开“个人中心”页面。
2. 在“密码管理”部分，“当前密码”字段中输入当前有效密码。
3. 在“新密码”和“确认密码”字段中输入新密码。
4. 点击【确定】按钮保存，下次登录时使用新密码。

|  |
| --- |
| 注意：  修改当前用户密码时，“当前密码”必须输入正确，否则无法更改密码。另外，“新密码”和“确认密码”输入必须一致，且符合密码复杂度要求，否则无法更改密码。 |

### 用户管理

系统用户即系统管理用户。

#### 新建本地用户

新建本地用户操作步骤如下：

1. 选择“系统”>“用户管理”菜单，点击【新建】按钮。系统将显示“本地用户”页面。
2. 在 “本地用户”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 用户类型 | 系统缺省显示为“本地用户”。 |
| 用户名 | 系统登录账号，登陆帐号必须为“3-12位数字、字母、下划线”组成的字符，区分大小写，不能包含反斜杠(\)，且不允许重名。 |
| 姓名 | 与用户名对应的员工姓名。 |
| 密码 | 与用户名对应的登陆密码。 |
| 确认密码 | 再一次确认密码 |
| 邮箱 | 新建用户的电子邮件地址。该地址必须真实有效，当新建用户成功后，系统将发送邮件到该邮箱地址，邮件内容描述该用户的密码认证认证信息。邮箱地址不允许重复。 |
| 密码发送 | 是否使用邮箱发送注册密码。 |
| 部门 | 当前新建用户所属的“组织资源”。 |
| 角色 | 管理员所属的角色类型，包括：系统管理员、安全管理员、安全审核员。 |
| 失效时间 | 定义该用户失去在其权限范围内操作系统的时间。 |
| 备注 | 备注描述信息 |
| 信任主机 | 添加信任主机，该用户只能在信任主机（IP）下正常访问系统 |

#### 编辑用户

用于修改用户信息。操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择待编辑的用户，点击【修改】按钮。
2. 在“本地用户”页面，按指定要求输入信息，点击【确定】保存。

#### 删除用户

从用户列表删除用户。操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择待删除的记录，点击【删除】按钮。
2. 在提示窗口，点击【确定】保存。

|  |
| --- |
| 注意：  删除某个用户时，将同时删除该用户保存的报表。 |

#### 密码重置

当用户密码丢失且无法恢复时，可通过密码重置功能为用户分配新密码。重置密码后，用户的新密码将会发送到用户注册时登记的邮箱!

操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择需要密码重置的用户，点击【重置密码】按钮。
2. 在提示窗口，点击【确定】保存。

#### 用户查询

系统提供按“用户名”、“姓名”、“备注”、“角色”、“用户来源”的模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“用户管理”菜单，查询条件中输入“用户名”、或“姓名”、或“备注”、或“角色”、或“用户类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 角色管理

**管理系统用户的所属角色，为角色分配用户和权限。提供新建角色、修改角色、删除角色功能。**

**系统中内置三种默认角色：系统管理员（sysadmin）、安全管理员（secadmin）、安全审核员（adtadmin）。**

* 系统管理员

**此角色提供对系统管理中“系统”模块及相关菜单选项的访问权限。系统管理员的操作权限有：查看状态模块的“系统信息”**、**“系统状态”**、**“系统告警”等信息；管理系统内的组织资源、用户管理、认证设置、告警管理、数据备份/恢复、许可管理、基本设置、网络管理等信息。**

**注意，系统管理员角色中的用户不具备查看详细的事件信息或创建策略等操作权限。**

* 安全管理员

**安全管理员可以配置规则、策略，跟踪事件、报表统计分析、风险趋势做出响应分析等。**

**此角色授予用户管理业务资源、**物理资源**、**数据资源**、高级资源、**规则**、网络**防护策略、网络防护规则管理、网络防护事件**、网络防护**报表**、**任务中心**等模块及相关菜单选项的访问的权限。**

* 安全审核员

**安全审核员提供对系统中“审计”模块、角色管理模块及相关菜单选项的访问权限，此角色中的用户可以查看系统告警信息。**

#### **新建角色**

操作步骤如下：

1. 选择“系统”>“角色管理”菜单，点击【新建】按钮。
2. 在“系统”>“角色管理”>“角色信息”页面，按指定要求输入信息，以及选择要定义的使用和管理权限，点击【确定】保存。

* 角色名称：角色的名称。
* 角色描述：角色的简要描述说明。
* 权限：指定该角色所要授予的访问和使用权限。

#### 编辑角色

用于修改角色信息。操作步骤如下：

1. 选择“系统”>“角色管理”菜单，选择待编辑的记录，点击“修改”按钮。
2. 在“系统”>“用户管理”>“角色信息”页面，按指定要求输入信息，并勾选所需要访问权限的模块，点击【确定】保存。

#### 删除角色

用于删除角色信息。操作步骤如下：

1. 选择“系统”>“角色管理”菜单，选择待删除的记录，点击【删除】按钮。
2. 在“确定要删除已选择的角色吗?”提示窗口，点击【确定】按钮。

|  |
| --- |
| 注意：   * 当存在用户与角色相关联时，不允许删除该角色。 * 系统预定义的角色不可删除。 |

#### 角色查询

系统提供按“角色名称”、“角色描述”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“角色管理”菜单，查询条件中输入“角色名称”、或“角色描述”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 安全日志维护

用于管理和维护安全日志，提供“安全日志”的归档、恢复、删除等维护功能。

#### 归档

操作步骤如下：

1. 点击“系统”>“安全日志维护”菜单。
2. 在“安全日志维护”页面，点击【归档】按钮。
3. 在“归档”页面，按指定要求输入信息，点击【确定】按钮保存。

* 开始时间、结束时间：（\*）选择要归档的系统日志的开始时间。
* 是否删除原纪录：该项默认选择“是”，表示将“安全日志”以文件形式归档时删除数据库中的系统操作日志记录。此处的删除指“完全删除”。

选择“否”，表示系统日志以文件形式归档时不删除数据库中的系统操作日志记录。

* 备注：输入归档时的可选备注信息。

#### 恢复归档

用于恢复已归档的“安全日志”。恢复后，安全日志将重新插入至数据库中。

操作步骤如下：

1. 点击“系统”>“安全日志维护”菜单。
2. 在“安全日志维护”页面，选择恢复的日志记录，点击【恢复】按钮。

#### 删除归档

用于删除归档记录。删除列表中的归档记录时，同时删除对应的归档文件，但不删除数据库中已恢复的安全日志。

操作步骤如下：

1. 点击“系统”>“安全维护”菜单。
2. 在“安全日志维护”页面，选择待删除的记录，点击【删除】按钮。在提示窗口中，点击【确定】按钮确认删除。此处删除指删除“归档记录”和“归档文件”，与数据库中的“安全日志”记录无关。

#### 排序

对安全日志维护列表的数据进行排序。您可以单击表格中任意列标题上的▼或▲箭头将它们排序（升序或降序）。

#### 安全日志维护查询

系统提供按“状态”、“开始时间”、“操作时间”、“结束时间”、模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“安全日志维护”菜单，查询条件中输入“状态”、 “开始时间”、“操作时间”、“结束时间”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 密码安全策略设置

用于管理用户的密码策略,保证密码的安全级别。

* + - 1. 选择“系统”>“密码安全策略设置”菜单。
      2. 在“密码安全策略设置”页面，选择相关的密码安全策略，点击【确定】按钮保存。

### 信任主机管理

“信任主机”是指可以访问系统的主机，如不在信任主机列表的主机将不允许访问系统。

#### 新建信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，点击【信任主机添加】选项卡。
2. 在“信任主机列表”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 名称 | 该主机的名称 |
| 主机IP | 该主机的IP地址 |

#### 编辑信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，选择待编辑的信任主机。
2. 在该记录的最右侧点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，选择待删除的信任主机记录。
2. 点击该记录右侧的【🗑删除】按钮，在提示窗口，点击【确定】保存。

#### 信任主机模糊查询

系统提供按“名称”、“信任IP”、“备注”模糊 查询功能。

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，查询条件中输入“名称”、“信任IP”、“备注”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

## 安全审核员

安全审核员有权限查看生成的事件、报表，并对日志进行维护。

作为安全审核员，具备以下权限：

* 权限管理：“个人中心”、“角色管理”、“用户管理”
* 数据管理：“系统操作日志”、“日志维护”
* 告警管理：“告警管理”
* 系统设置：“信任主机管理”

以下将对上述功能分别进行描述

### 个人中心

#### 查看用户信息

选择“系统”>“个人中心”菜单，显示当前登录用户的详细信息，包括用户名、电子邮箱地址、当前用户的所属角色。

#### 向导设置

* 自动显示向导：指用户首次登录系统时，系统自动弹出“向导帮助”页面，引导用户使用系统。
* 手动显示向导：指用户首次登录系统时，系统不弹出“向导帮助”页面，如需要使用向导功能，需点击系统页面右上角的【向导】按钮，来进入“向导帮助”页面。

#### 更改密码

修改当前登录用户的密码。操作步骤如下：

1. 点击“系统”>“个人中心”菜单，将打开“个人中心”页面。
2. 在“密码管理”部分，“当前密码”字段中输入当前有效密码。
3. 在“新密码”和“确认密码”字段中输入新密码。
4. 点击【确定】按钮保存，下次登录时使用新密码。

|  |
| --- |
| 注意：  修改当前用户密码时，“当前密码”必须输入正确，否则无法更改密码。另外，“新密码”和“确认密码”输入必须一致，且符合密码复杂度要求，否则无法更改密码。 |

### 用户管理

系统用户即系统管理用户。

#### 新建本地用户

新建本地用户操作步骤如下：

1. 选择“系统”>“用户管理”菜单，点击【新建】按钮。系统将显示“本地用户”页面。
2. 在 “本地用户”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 用户类型 | 系统缺省显示为“本地用户”。 |
| 用户名 | 系统登录账号，登陆帐号必须为“3-12位数字、字母、下划线”组成的字符，区分大小写，不能包含反斜杠(\)，且不允许重名。 |
| 姓名 | 与用户名对应的员工姓名。 |
| 密码 | 与用户名对应的登陆密码。 |
| 确认密码 | 再一次确认密码 |
| 邮箱 | 新建用户的电子邮件地址。该地址必须真实有效，当新建用户成功后，系统将发送邮件到该邮箱地址，邮件内容描述该用户的密码认证认证信息。邮箱地址不允许重复。 |
| 密码发送 | 是否使用邮箱发送注册密码。 |
| 部门 | 当前新建用户所属的“组织资源”。 |
| 角色 | 管理员所属的角色类型，包括：系统管理员、安全管理员、安全审核员。 |
| 失效时间 | 定义该用户失去在其权限范围内操作系统的时间。 |
| 备注 | 备注描述信息 |
| 信任主机 | 添加信任主机，该用户只能在信任主机（IP）下正常访问系统 |

#### 编辑用户

用于修改用户信息。操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择待编辑的用户，点击【修改】按钮。
2. 在“本地用户”页面，按指定要求输入信息，点击【确定】保存。

#### 删除用户

从用户列表删除用户。操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择待删除的记录，点击【删除】按钮。
2. 在提示窗口，点击【确定】保存。

|  |
| --- |
| 注意：  删除某个用户时，将同时删除该用户保存的报表。 |

#### 密码重置

当用户密码丢失且无法恢复时，可通过密码重置功能为用户分配新密码。重置密码后，用户的新密码将会发送到用户注册时登记的邮箱!

操作步骤如下：

1. 选择“系统”>“用户管理”菜单，选择需要密码重置的用户，点击【重置密码】按钮。
2. 在提示窗口，点击【确定】保存。

#### 用户查询

系统提供按“用户名”、“姓名”、“备注”、“角色”、“用户来源”的模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“用户管理”菜单，查询条件中输入“用户名”、或“姓名”、或“备注”、或“角色”、或“用户类型”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 角色管理

**管理系统用户的所属角色，为角色分配用户和权限。提供新建角色、修改角色、删除角色功能。**

**系统中内置三种默认角色：系统管理员（sysadmin）、安全管理员（secadmin）、安全审核员（adtadmin）。**

* 系统管理员

**此角色提供对系统管理中“系统”模块及相关菜单选项的访问权限。系统管理员的操作权限有：查看状态模块的“系统信息”**、**“系统状态”**、**“系统告警”等信息；管理系统内的组织资源、用户管理、认证设置、告警管理、数据备份/恢复、许可管理、基本设置、网络管理等信息。**

**注意，系统管理员角色中的用户不具备查看详细的事件信息或创建策略等操作权限。**

* 安全管理员

**安全管理员可以配置规则、策略，跟踪事件、报表统计分析、风险趋势做出响应分析等。**

**此角色授予用户管理业务资源、**物理资源**、**数据资源**、高级资源、**规则**、网络**防护策略、网络防护规则管理、网络防护事件**、网络防护**报表**、**任务中心**等模块及相关菜单选项的访问的权限。**

* 安全审核员

**安全审核员提供对系统中“审计”模块、角色管理模块及相关菜单选项的访问权限，此角色中的用户可以查看系统告警信息。**

#### **新建角色**

操作步骤如下：

1. 选择“系统”>“角色管理”菜单，点击【新建】按钮。
2. 在“系统”>“角色管理”>“角色信息”页面，按指定要求输入信息，以及选择要定义的使用和管理权限，点击【确定】保存。

* 角色名称：角色的名称。
* 角色描述：角色的简要描述说明。
* 权限：指定该角色所要授予的访问和使用权限。

#### 编辑角色

用于修改角色信息。操作步骤如下：

1. 选择“系统”>“角色管理”菜单，选择待编辑的记录，点击“修改”按钮。
2. 在“系统”>“用户管理”>“角色信息”页面，按指定要求输入信息，并勾选所需要访问权限的模块，点击【确定】保存。

#### 删除角色

用于删除角色信息。操作步骤如下：

1. 选择“系统”>“角色管理”菜单，选择待删除的记录，点击【删除】按钮。
2. 在“确定要删除已选择的角色吗?”提示窗口，点击【确定】按钮。

|  |
| --- |
| 注意：   * 当存在用户与角色相关联时，不允许删除该角色。 * 系统预定义的角色不可删除。 |

#### 角色查询

系统提供按“角色名称”、“角色描述”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“角色管理”菜单，查询条件中输入“角色名称”、或“角色描述”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 日志维护

提供“操作日志”的归档、恢复、删除等维护功能。

#### 归档

操作步骤如下：

1. 点击“系统”>“日志维护”菜单。
2. 在“日志维护”页面，点击【归档】按钮。
3. 在“归档”页面，按指定要求输入信息，点击【确定】按钮保存。

* 开始时间、结束时间：（\*）选择要归档的系统日志的开始时间。
* 是否删除原纪录：该项默认选择“是”，表示将“系统操作日志”以文件形式归档时删除数据库中的系统操作日志记录。此处的删除指“完全删除”。

选择“否”，表示系统日志以文件形式归档时不删除数据库中的系统操作日志记录。

* 备注：输入归档时的可选备注信息。

#### 恢复归档

用于恢复已归档的“系统操作日志”。恢复后，系统操作日志将重新插入至数据库中。

操作步骤如下：

1. 点击“系统”>“日志维护”菜单。
2. 在“日志维护”页面，选择恢复的日志记录，点击【恢复】按钮。

#### 删除归档

用于删除归档记录。删除列表中的归档记录时，同时删除对应的归档文件，但不删除数据库中已恢复的系统操作日志。

操作步骤如下：

1. 点击“系统”>“日志维护”菜单。
2. 在“日志维护”页面，选择待删除的记录，点击【删除】按钮。在提示窗口中，点击【确定】按钮确认删除。此处删除指删除“归档记录”和“归档文件”，与数据库中的“系统操作日志”记录无关。

#### 排序

对系统日志维护列表的数据进行排序。您可以单击表格中任意列标题上的▼或▲箭头将它们排序（升序或降序）。

#### 日志维护查询

系统提供按“状态”、“开始时间”、“操作时间”、“结束时间”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“日志维护”菜单，查询条件中输入状态”、“开始时间”、“操作时间”、“结束时间”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 系统操作日志

系统操作日志显示所有登录用户所执行的系统操作。包括执行系统操作时的时间、用户帐号、所属角色、操作记录。

#### 系统操作日志查询

系统提供按“用户”、“角色”、“操作”、“时间”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“系统操作日志”菜单，查询条件中输入“用户”、或“角色”等信息，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 告警管理

点击“系统”>“告警管理”菜单，“告警管理”页面会向用户显示系统告警信息， “告警管理”分为“历史告警”、“实时告警”和“告警统计”三个功能模块。

#### 历史告警

历史告警显示历次系统告警信息，告警信息最多显示最近10万条记录，超出10万限制，系统删除最早的记录。

* 告警名称：显示当前记录的告警名称，包括CPU告警、内存告警、存储告警。
* 告警类型：显示当前记录的告警类型，包括系统告警。
* 系统告警：指CPU、内存、存储告警、登陆异常告警。
* 告警级别：告警级别分为提示、一般、严重、重要、紧急五类。
* 提示：当CPU、内存、存储达到指定阈值，触发提示告警。
* 一般：当CPU、内存、存储达到指定阈值，触发一般告警。
* 严重：当CPU、内存、存储达到指定阈值，触发严重告警。
* 重要：当CPU、内存、存储达到指定阈值，触发重要告警。
* 紧急：当CPU、内存、存储达到指定阈值，触发紧急告警。
* 捕获时间：显示触发告警的具体时间。
* 告警描述：显示告警记录的描述内容及解除告警的办法。
* 告警状态：显示告警是否已被管理员确认。
* 操作：对告警进行确认操作。
* 告警详细信息：显示告警记录的详细内容，内容包括告警名称、告警级别、告警触发条件、告警捕获时间、告警描述。

#### 实时告警

实时告警显示当前时间最近的15条告警信息。

* 告警名称：显示告警类型，包括CPU告警、内存告警、存储告警。
* 告警级别：告警级别分为提示、一般、严重、重要、紧急五类。
* 提示：当CPU、内存、存储达到指定阈值，触发提示告警。
* 一般：当CPU、内存、存储达到指定阈值，触发一般告警。
* 严重：当CPU、内存、存储达到指定阈值，触发严重告警。
* 重要：当CPU、内存、存储达到指定阈值，触发重要告警。
* 紧急：当CPU、内存、存储达到指定阈值，触发紧急告警。
* 捕获时间：显示触发告警的具体时间。
* 告警描述：显示告警记录的描述内容及解除告警的办法。
* 告警状态：显示告警是否已被管理员确认。
* 操作：对告警进行确认操作。
* 告警详细信息：显示告警记录的详细内容，内容包括告警名称、告警级别、告警触发条件、告警捕获时间、告警描述。

|  |
| --- |
| 注：  【确认】某告警信息，此信息就不会在‘历史告警’、‘实时告警’列表中展现，但会在‘告警统计’中统计 |

#### 告警统计

告警统计能够根据条件显示告警趋势图。

* 告警统计条件：
* 告警级别：告警级别分为提示、一般、严重、重要、紧急五类，支持全选或多选。
* 告警状态：告警状态分为“确认”和“未确认”两种。
* 告警触发条件：选择告警统计的分组方式，例如： CPU、内存、存储。
* 时间粒度：选择告警统计的时间粒度，例如：最近一月、最近一周、天、自定义。当选择自定义时，系统显示起始时间、结束时间页面。

起始时间：统计告警信息的起始时间。

结束时间：统计告警信息的结束时间。

* 查询：根据定义的起始时间显示告警趋势图。
* 重置：重置告警统计条件。

#### 告警查询

系统提供按“告警名称”、“告警描述”、 “告警级别”、“捕获时间”模糊查询功能，支持组合查询。

操作步骤如下：

1. 选择“系统”>“告警管理”菜单，在“历史告警”选项卡或“实时告警”选项卡中，查询条件中输入“告警名称”、或“告警描述”、或“告警级别”、或“捕获时间”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。

### 信任主机管理

“信任主机”是指可以访问系统的主机，如不在信任主机列表的主机将不允许访问系统。

#### 新建信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，点击【信任主机添加】选项卡。
2. 在“信任主机列表”页面，按指定要求输入信息，点击【确定】保存。

界面上各参数的说明解释请参见下表。

|  |  |
| --- | --- |
| 参数 | 说明 |
| 名称 | 该主机的名称 |
| 主机IP | 该主机的IP地址 |

#### 编辑信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，选择待编辑的信任主机。
2. 在该记录的最右侧点击【修改】按钮，按指定要求输入信息，点击【确定】保存。

#### 删除信任主机

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，选择待删除的信任主机记录。
2. 点击该记录右侧的【删除】按钮，在提示窗口，点击【确定】保存。

#### 信任主机模糊查询

系统提供按“名称”、“信任IP”、“备注”模糊查询功能。

操作步骤如下：

1. 选择“系统”>“信任主机管理”菜单，在“信任主机列表”选项卡中，查询条件中输入“名称”、“信任IP”、“备注”，点击【查询】按钮。
2. 点击【重置】按钮，将查询条件清空。