

---

# 天融信日志收集与分析系 统 一本通（企业版）

---

# Table of Contents

1. 欢迎使用 .....	4
1.1 约定 .....	4
1.2 技术服务体系 .....	5
2. 系统简介 .....	6
2.1 系统组成 .....	6
2.2 系统功能 .....	7
3. 安装 .....	8
3.1 规划与部署 .....	8
3.2 安装天融信日志收集与分析系统 .....	9
3.2.1 安装 TA-L 服务器 .....	10
3.2.1.1 安装环境 .....	10
3.2.1.2 安装服务器 .....	10
3.2.1.2.1 管理节点 .....	10
3.2.1.2.2 下级节点 .....	17
3.2.2 安装收集代理 .....	24
3.2.2.1 安装环境 .....	24
3.2.2.2 安装代理 .....	24
3.2.3 安装告警节点 .....	30
3.2.3.1 安装环境 .....	30
3.2.3.2 安装告警程序 .....	30
3.3 启动天融信日志收集与分析系统 .....	36
3.3.1 系统服务启动方式 .....	36
3.3.2 应用程序启动方式 .....	40
3.3.3 登录 TA-L 系统 .....	42
3.4 关闭天融信日志收集与分析系统 .....	43
3.5 卸载天融信日志收集与分析系统 .....	45
4. 初次使用系统 .....	45
4.1 系统登录 .....	45
4.2 系统用户 .....	47
5. 操作管理员 .....	47
5.1 主页 .....	48
5.2 日志 .....	59
5.2.1 日志摘要 .....	59
5.2.2 实时日志 .....	60
5.2.3 日志查询 .....	61
5.2.4 备份管理 .....	67
5.2.4.1 日志备份 .....	67
5.2.4.2 备份导入 .....	68
5.2.5 查询统计 .....	69
5.2.5.1 统计主题 .....	70
5.2.5.2 统计任务 .....	72

---

5.3 报表.....	75
5.3.1 基本报表.....	76
5.3.1.1 系统报表.....	76
5.3.1.2 告警报表.....	80
5.3.1.2.1 告警报表.....	81
5.3.1.2.2 告警趋势.....	85
5.3.1.3 日志报表.....	87
5.3.2 计划报表.....	89
5.4 告警.....	92
5.4.1 告警摘要.....	92
5.4.2 实时告警.....	94
5.4.3 告警查询.....	96
5.5 日志源.....	97
5.5.1 日志源管理.....	97
5.5.2 业务组.....	102
5.6 知识库.....	104
5.7 配置.....	106
5.7.1 存储管理.....	106
5.7.1.1 存储策略.....	106
5.7.1.2 备份策略.....	107
5.7.2 转发配置.....	110
5.7.2.1 Syslog 转发.....	110
5.7.2.2 JMS 转发.....	112
5.7.3 系统配置.....	114
5.7.3.1 日志过滤规则.....	114
5.7.3.2 告警规则.....	116
5.7.3.3 告警过滤规则.....	121
5.7.3.4 告警方式管理.....	122
5.7.3.5 邮件服务器.....	130
5.7.3.6 采集器端口.....	131
5.7.3.7 节点管理.....	132
5.7.3.8 系统备份.....	135
5.7.3.9 资源管理.....	136
5.7.3.10 设备支持列表.....	137
5.8 关于.....	137
5.9 锁定.....	140
6. 审计管理员.....	141
6.1 主页.....	141
6.2 日志.....	142
6.3 报表.....	142
6.3.1 基本报表.....	143
6.3.2 计划报表.....	147
7. 账户管理员.....	150
7.1 主页.....	150

---

7.2 用户 .....	151
7.2.1 用户管理 .....	151
7.2.2 安全管理 .....	154

---

# 1. 欢迎使用

## ●前言

---

天融信日志收集与分析系统（TA-L）是集日志收集、存储、分析和统计于一体的专业日志审计系统。本文档主要介绍了天融信日志收集与分析系统的系统架构、安装、使用和管理，通过阅读本文档，用户可以了解系统的基本组成，并能够正确地配置使用系统，对日志进行多维度的综合分析，实现对网络中日志源设备的全方位安全监管。

## ●软件版本

---

V3.3.3.10【企业版】

## ●文档意见反馈

---

如果您在阅读过程中发现文档的任何问题，可通过服务热线或电子邮件（[plm\\_prm\\_doc@topsec.com.cn](mailto:plm_prm_doc@topsec.com.cn)）的方式进行反馈。感谢您的反馈，让我们做得更好！

## ●声明

---

1. 本文档中所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。
2. 本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。
3. 本文档中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
4. 本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。


## 1.1 约定

本文档遵循以下约定：

- 1) 图形界面操作的描述采用以下约定：

格式	说明
【XX】	表示按钮。如：点击【XX】按钮。
“”	表示页面内容引用。如：激活“XX”页签，弹出“XX”窗口，在下拉框中选择“XX”参数。
>	分隔多个菜单项，且此时菜单项采用“菜单命令”格式。 如：点击（选择） <b>系统管理 &gt; 通讯管理</b> 。
< >	带尖括号表示键盘按钮名。如：按 <Ctrl> + <Alt> 即可。

2) 文档中出现的说明、注意、示例等标志，是关于用户在配置互联网接入口检测器过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。这些标志的意义如下：

格式	说明
	“说明”图标，对操作内容的描述进行必要的补充和说明。
	“注意”图标，提醒操作中应注意的事项，不当的操作可能会导致数据丢失或设备损坏。
	“示例”图标，对相关描述进行举例说明。

## 1.2 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

<http://www.topsec.com.cn> (See 1.2)

## 2. 系统简介

天融信日志收集与分析系统（TA-L）是一个跨平台的日志审计系统。该系统通过收集网络中的各种网络设备、安全设备（包括但不限于防火墙、IDS 系统、VPN 和防病毒系统）、主机系统（即 Windows 和 Unix/Linux）、应用服务（包括但不限于 Mail 服务、Web 服务、FTP 服务和 DNS 服务）等产生的大量日志数据，进行集中管理和全面、有效的综合统计，为用户提供了一个方便、高效、直观的日志安全审计平台，能够帮助用户及时发现网络中存在的安全风险、准确地进行事后取证，进而可以更加有效地保障自身网络的安全运行。

相关内容包括：

- [系统组成](#) (See 2.1)
- [系统功能](#) (See 2.2)

### 2.1 系统组成

天融信日志收集与分析系统主要由七个子系统组成。



天融信日志收集与分析系统组成

- 日志采集子系统

日志采集子系统是整个系统的基础，负责收集各种设备、应用的日志。支持服务器直接采集和通过外部代理采集两种方式，适应不同的设备和应用日志。

- 日志处理子系统

日志处理子系统负责将收集到的各种格式日志进行解析、归一化处理，提供给后续模块进行分析存储。

- 日志管理子系统

管理该系统收集到的所有日志，包括系统自身产生的审计日志。支持日志的实时监视、查询、备份、导出管理。

---

- 日志存储子系统

日志存储子系统支持存储系统收集到的所有日志。支持按照存储时间和空间多个维度的策略进行管理，支持海量日志管理。

- 统计分析子系统

统计分析子系统支持实时统计分析，系统通过预置的上百种统计规则，实时统计分析收集到的日志。支持按照日、周、月、年等周期统计、展示日志分析结果。统计分析结果支持 word、pdf 等多种导出格式。

- 告警响应子系统

告警响应子系统能够根据规则对特定日志触发告警和响应动作。除了系统预置的告警规则外，支持用户自定义告警规则，方便用户监控系统的关键日志并做出及时处理。

- 管理子系统

管理子系统负责整个天融信日志收集与分析系统的配置与管理。包括系统参数配置、日志源管理等。

## 2.2 系统功能

### 日志收集

通过配置多种类型的日志源，天融信日志收集与分析系统能够支持安全设备、网络设备、操作系统及应用协议等多种日志数据的收集。

目前，天融信日志收集与分析系统支持的日志类型主要包括：

- 网络设备日志
- 安全设备日志
- 主机服务器日志
- 各种应用系统日志

### 日志存储

天融信日志收集与分析系统集中存储所有收集到的日志。

- 集中存储

集中存储可以提高日志的安全性并方便管理。支持灵活的存储策略，可以为不同日志源设置不同的存储策略。支持存储空间上限管理，当存储空间不足时会自动删除最旧的日志，优先存储最新产生的日志。

- 原始格式

天融信日志收集与分析系统同时存储格式化日志和原始日志，以便能够最大限度还原原始信息，为准确取证提供保障。

### 日志查询

天融信日志收集与分析系统提供了多样、灵活的日志信息查询功能，方便管理员快速查找定位关键日志和准确地进行事后取证。

- 条件查询



---

支持多条件组合查询日志数据，查询结果可以导出查看。如果不输入条件，默认查询所有该时间段内日志。查询结果倒序显示，也就是最近产生的日志在前面。

- 支持原始日志与格式化后日志对比显示

查询结果可以同时显示符合条件的原始日志和格式化日志，可以帮助管理员更详细了解日志信息。

- 查询结果可导出

日志查询结果可以导出到文件中，方便离线使用。

- 历史日志检索

备份的历史日志可以重新导入查询，目前支持按照导出日志文件为单位进行查询管理。

### 统计报表

天融信日志收集与分析系统支持实时统计报表，能够根据预置的各种报表模板实时生成统计报表数据，达到快速生成并展示报表的效果。系统根据各种设备日志类型预置了丰富的报表模板，并提供日、周、月、年等统计周期。查看统计分析结果不再需要漫长的等待。

### 实时监视

天融信日志收集与分析系统可以实时监视系统运行状态，包括 CPU、内存和磁盘空间使用率以及当前平均日志流量，方便管理员及时了解系统运行和负载情况，并能根据策略及时发出告警。

支持实时监视当前正在收集的日志。

### 告警响应

天融信日志收集与分析系统能够对系统状态和关键事件及时作出响应。目前支持邮件、SNMP trap、执行本地命令和声音等多种响应方式。

## 3. 安装

介绍天融信日志收集与分析系统（简称 TA-L）的安装和使用。用户可以了解如何正确地在网络中安装天融信日志收集与分析系统，并进行简单配置。

下面内容主要包括：

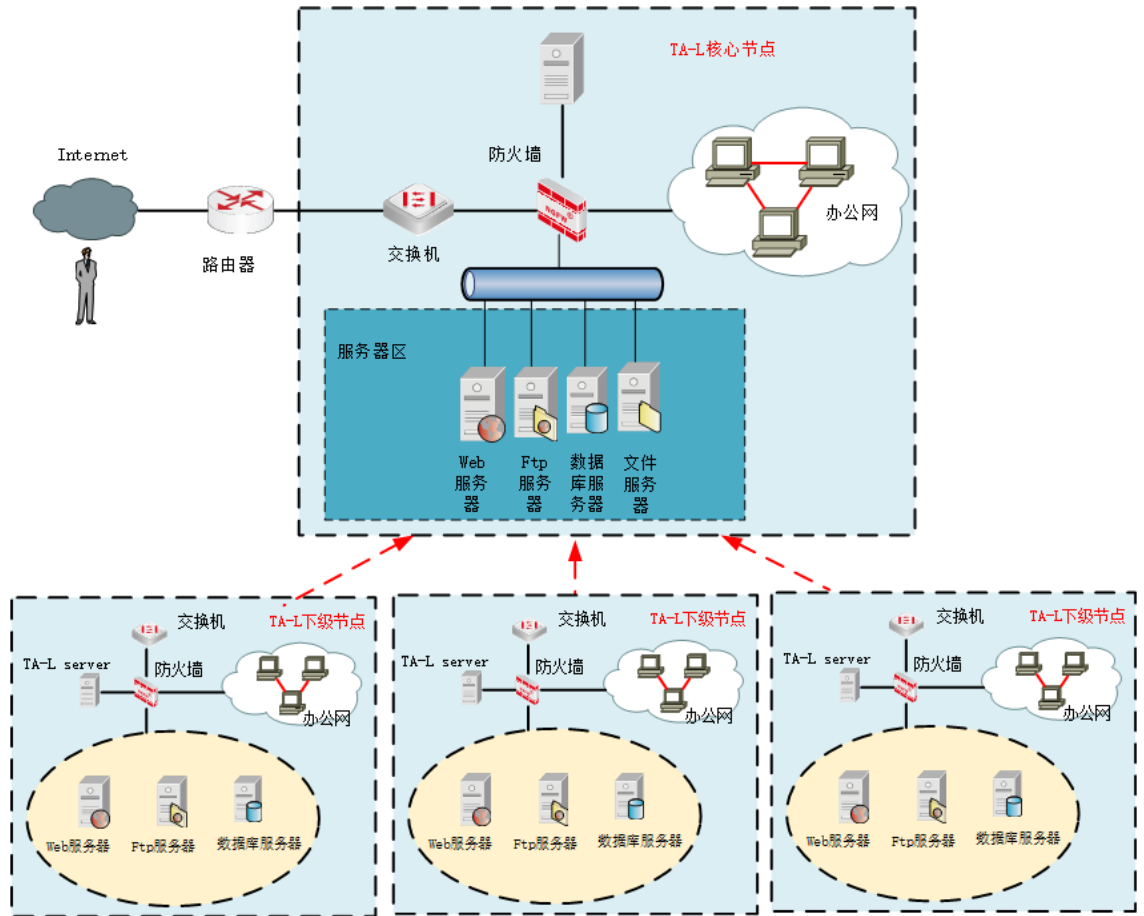
- [规划与部署](#) (See 3.1)
- [安装天融信日志收集与分析系统](#) (See 3.2)
- [启动天融信日志收集与分析系统](#) (See 3.3)
- [关闭天融信日志收集与分析系统](#) (See 3.4)
- [卸载天融信日志收集与分析系统](#) (See 3.5)

### 3.1 规划与部署

天融信日志收集与分析系统（以下简称 TA-L）是一个分布式、跨平台的安全审计系统。它可以对安全系统、网络设备、操作系统、应用系统等产生的日志信息进行统一收集、集中存储，并采用先进的智能信息处理技术对其进行综合分析。通过跨平台的日志收集、告警响应和全面的安全状

态分析等手段，TA-L 系统可以协助用户对已发生的安全风险进行取证、查询，为提高安全管理效率提供了有力的技术武器。

用户可以根据网络的整体规模、安全需求，以及日志流量等信息进行综合分析，合理部署天融信日志收集与分析系统。



上图描述了天融信日志收集与分析系统的多级部署情况。审计服务器收集日志信息的方式如下：

- 1) 每一级审计服务器直接收集防火墙、路由器和交换机等主动日志源的日志信息。
- 2) 审计服务器通过安装在远程服务器主机上的收集代理收集各种应用日志。
- 3) 下级服务器把检测出的安全事件上报给审计中心服务器。

## 3.2 安装天融信日志收集与分析系统

主要介绍天融信日志收集与分析系统在 Windows 平台下的服务器、收集代理的安装。（注意：建议不要将 TA-L 服务器与收集代理安装在同一台机器上。）

相关内容主要包括：

- [安装 TA-L 服务器](#) (See 3.2.1)
- [安装收集代理](#) (See 3.2.2)
- [安装告警节点](#) (See 3.2.3)

---

## 3.2.1 安装 TA-L 服务器

TA-L 服务器是天融信日志收集与分析系统的核心组成部分，是整个系统的支撑和管理平台。

### 3.2.1.1 安装环境

- 软件平台

操作系统：Windows 2008(64 位)企业版及以上版本

- 硬件平台

**最低配置：**

CPU：8 核以上处理器

内存：16G 以上

硬盘：1T

**推荐配置：**

CPU：XEON-8 核及以上处理器

内存：32GB 以上

硬盘：3TB 以上 RAID5 或者 RAID10，不推荐使用 RAID10

### 3.2.1.2 安装服务器

TA-L 服务器的安装类型主要分为管理节点和下级节点。具体安装类型依据部署环境，当部署环境为单级部署时，需要安装管理节点，只能部署一套。

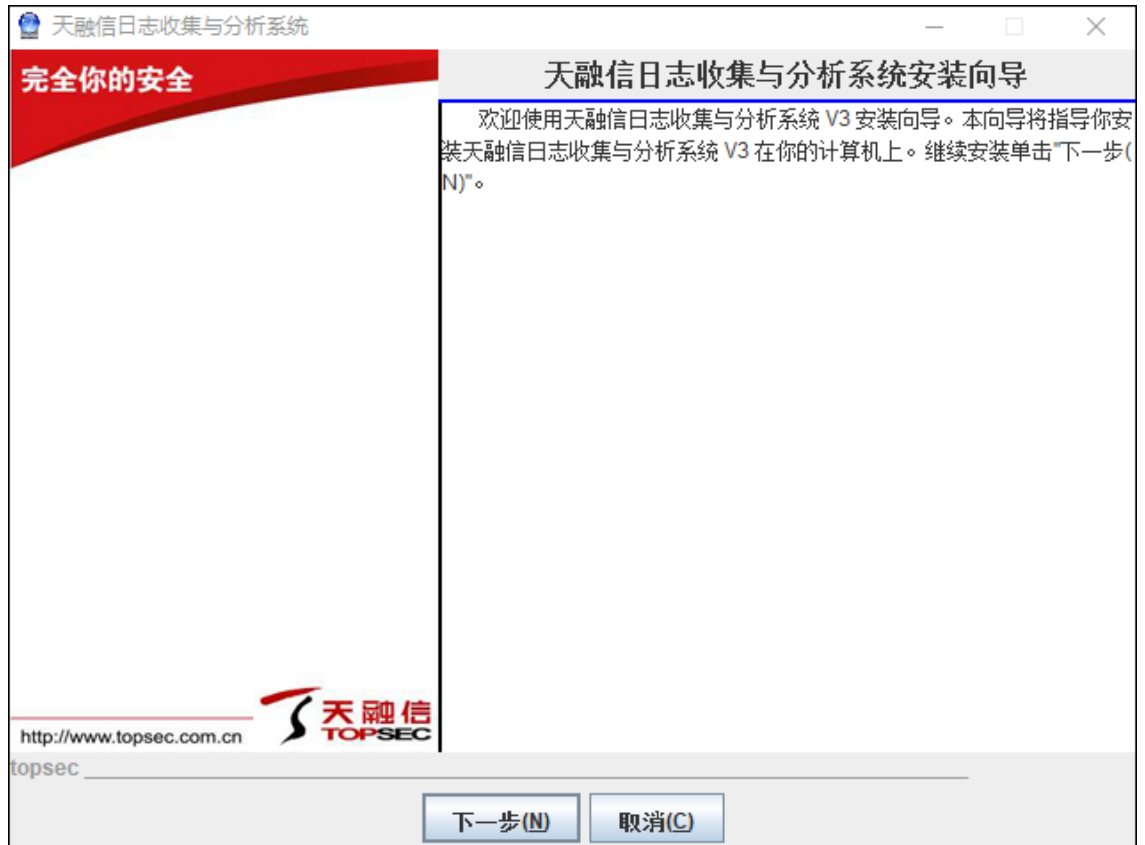
当部署环境为两级部署时，需要安装管理节点和下级节点，下级节点可以部署多套。

**需要说明的是**，管理节点和下级节点都需要安装在全新的操作系统上，不能跟其他应用或软件共用服务器。

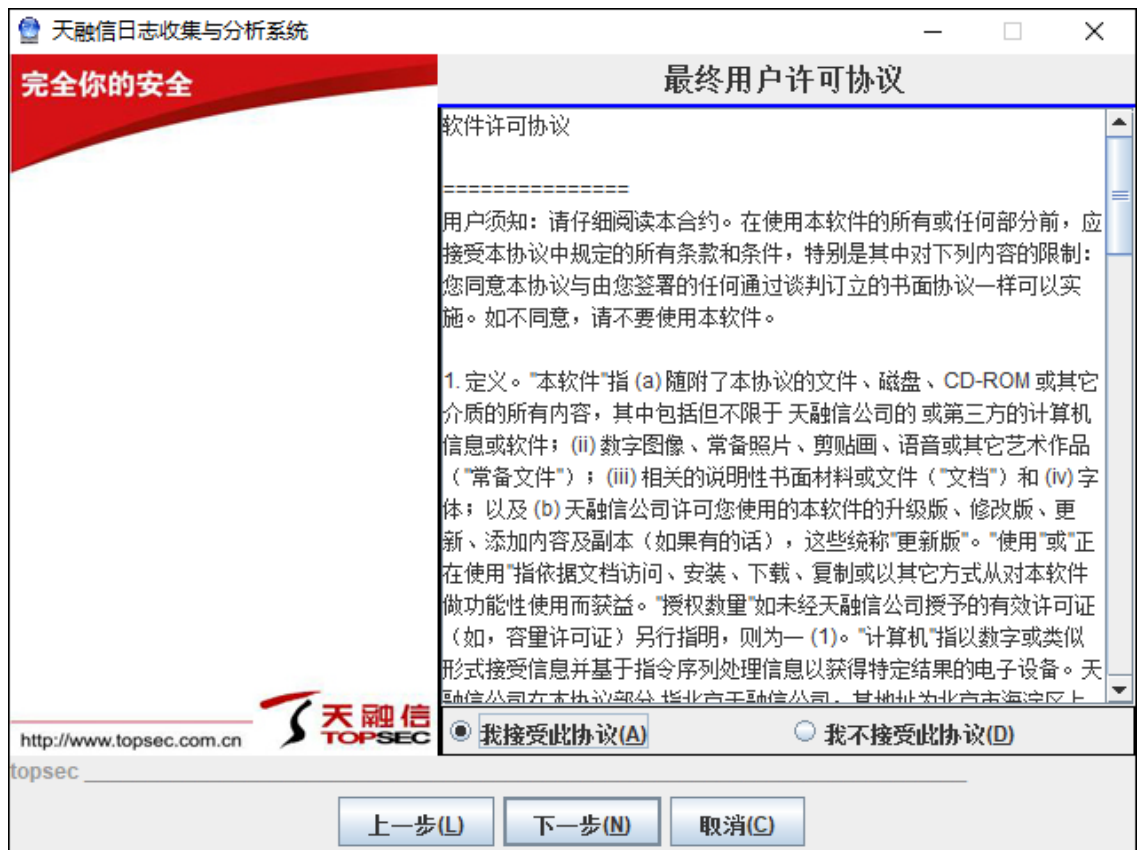
#### 3.2.1.2.1 管理节点

安装 TA-L 服务器管理节点的具体步骤如下：

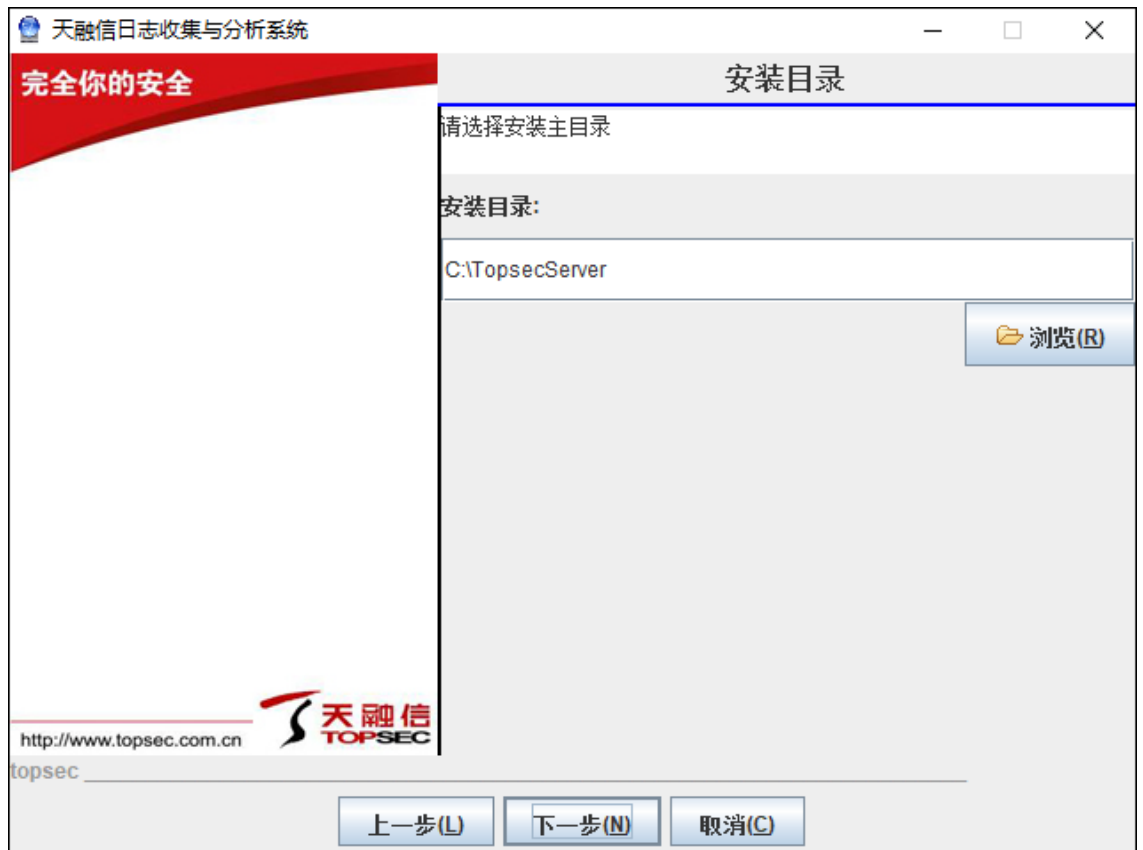
**步骤 1** 在安装光盘中，双击目录下的“setup.exe”，弹出如下图所示的窗口。



步骤 2 点击【下一步】按钮，接受最终用户许可协议，如下图所示。

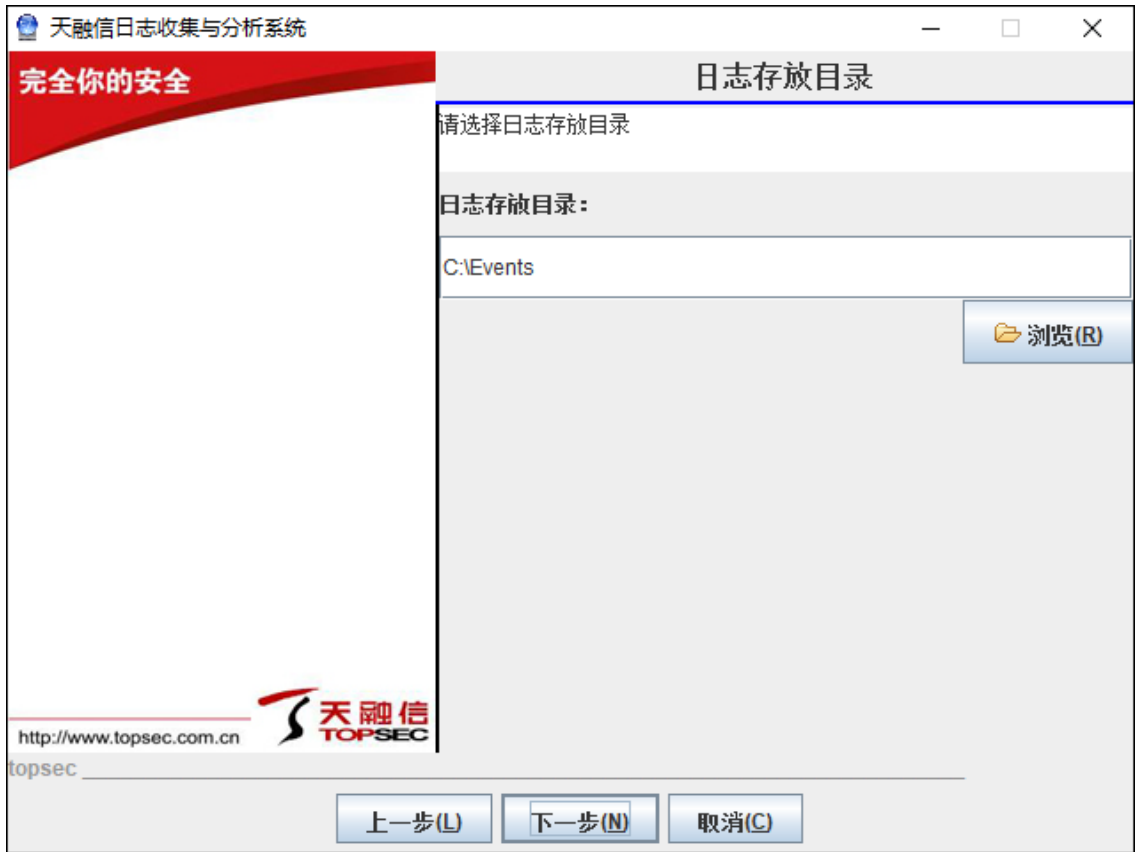


步骤 3 点击【下一步】按钮，设置安装目录。



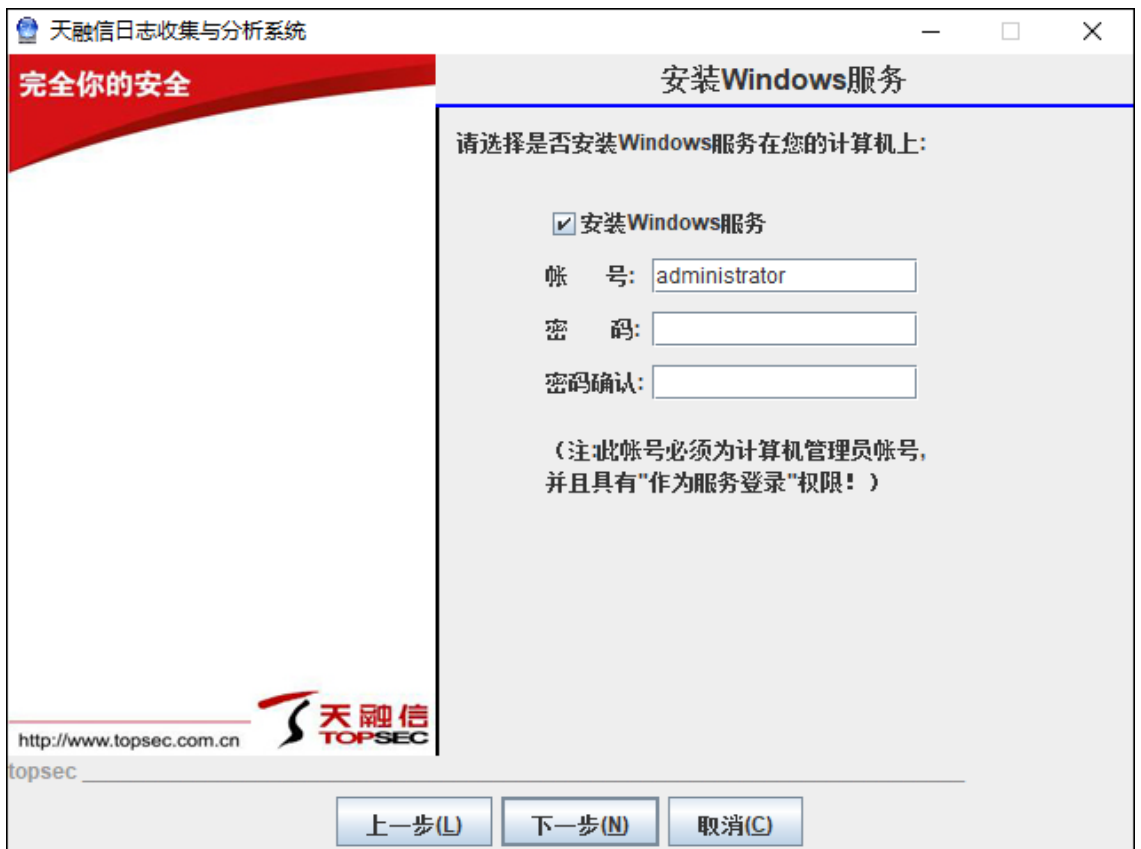
默认的安装目录为：C:\TopsecServer，用户可以通过点击【浏览】按钮改变安装目录，建议将系统安装在足够空间的非系统硬盘中。（注意：安装路径不支持中文和所有特殊字符）

步骤 4 点击【下一步】按钮，设置日志存放目录。



日志存放目录中将会存放大量的日志数据，建议选择较大的硬盘分区来存放日志。

**步骤 5** 点击【下一步】按钮，设置是否将 TA-L 安装为系统服务，如下图所示。



勾选“安装 Windows 服务”选项，输入计算机管理员帐号和密码并确认密码后，TA-L 服务器可以作为系统服务运行，服务名称为 TopAnalyzer。管理员可通过 **开始 > 程序 > 管理工具 > 服务** 对其进行启动和停止操作。

如果不勾选“安装 Windows 服务”选项，则不作为系统服务运行。安装完成后，可以通过 **开始 > 程序 > 天融信日志收集与分析系统 > 服务器** 来启动 TA-L 程序。

**步骤 6** 点击【下一步】按钮，选择安装的节点类型，选择安装管理节点，如下图所示。



TA-L 服务器支持两级部署模式，“管理节点”是指上级节点，只能部署一套，下级节点具体配置可参见 [下级节点](#) (See 3.2.1.2.2)。

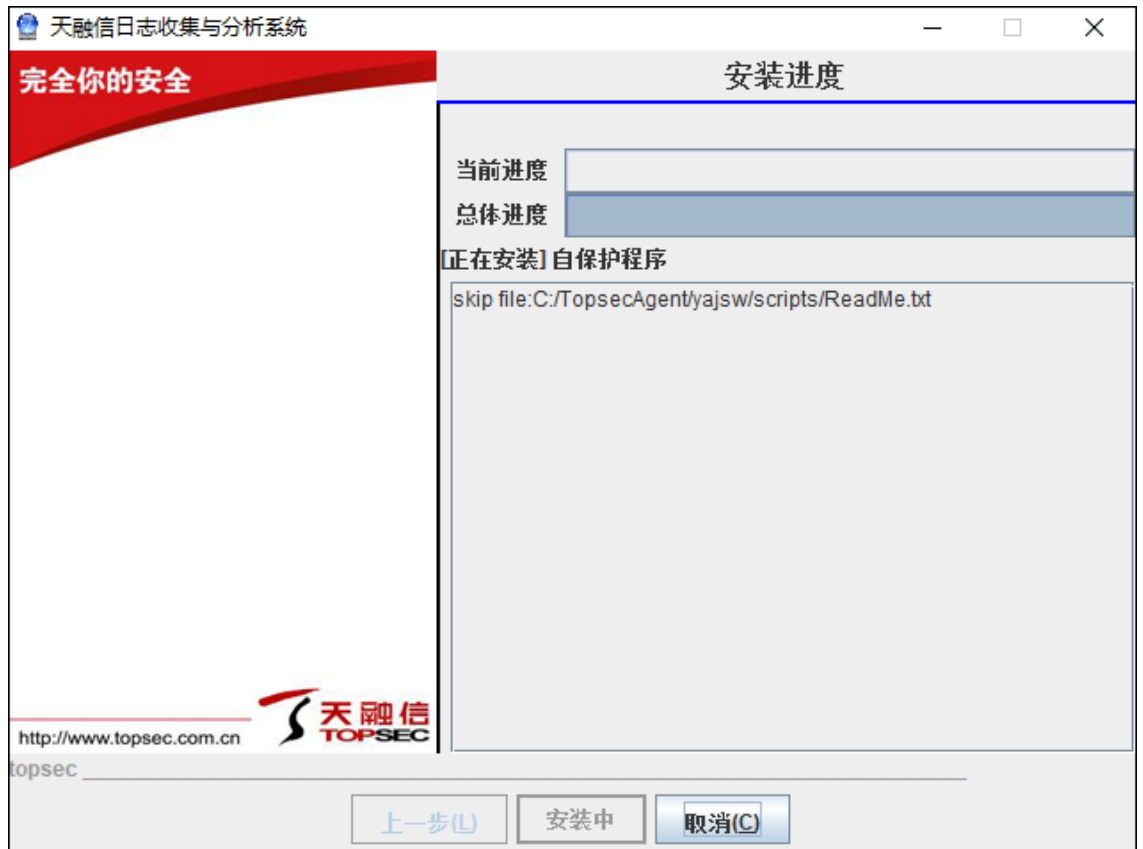
**步骤 7** 点击【下一步】按钮，导入备份文件，如下图所示。



此步骤通常适用于重新安装系统时，管理员可以在此将事先导出的系统配置文件导入，以省略安装后的配置。当用户第一次安装时，可以忽略此步骤，直接点击【下一步】按钮即可。

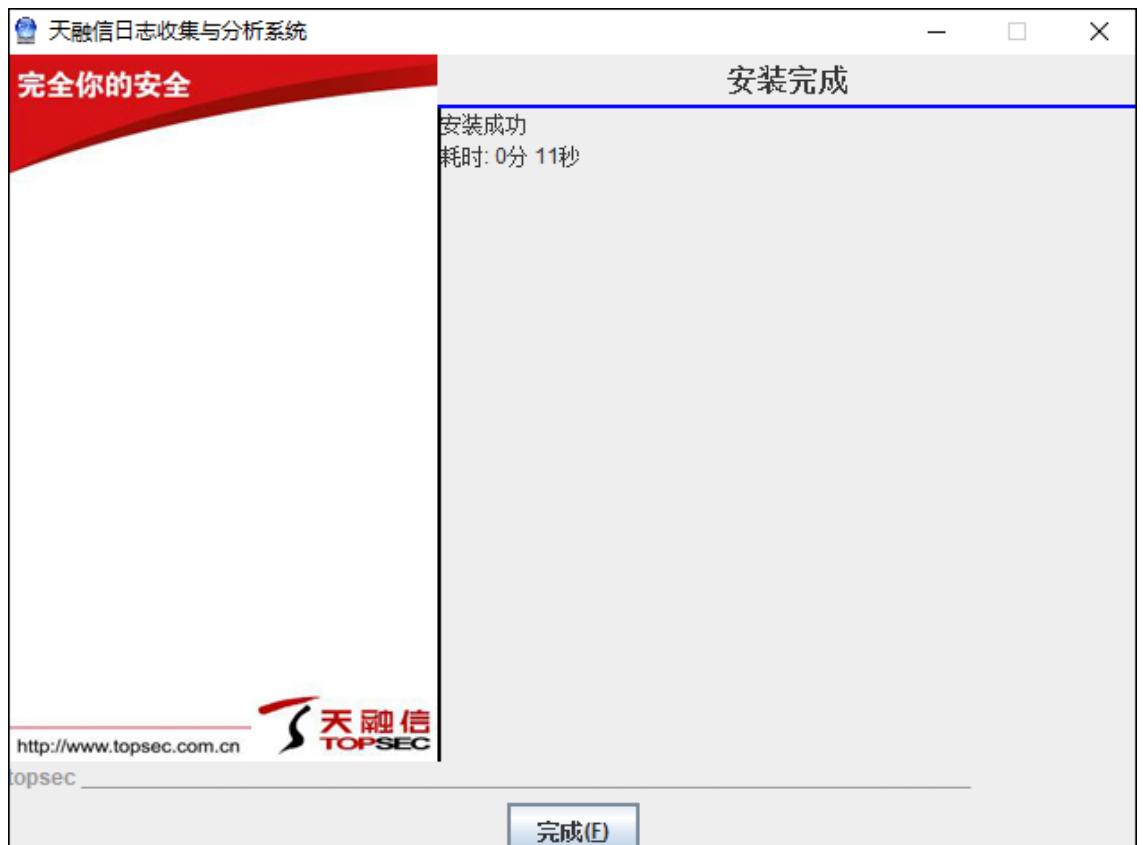
**步骤 8** 点击【下一步】按钮，开始 TA-L 服务器的安装，如下图所示。





TA-L 系统的整个安装过程根据机器性能情况，持续时间不同，请用户耐心等待。

**步骤 9** 安装完成后，点击【完成】按钮退出安装程序，如下图所示。



至此，TA-L 服务器的安装完成。

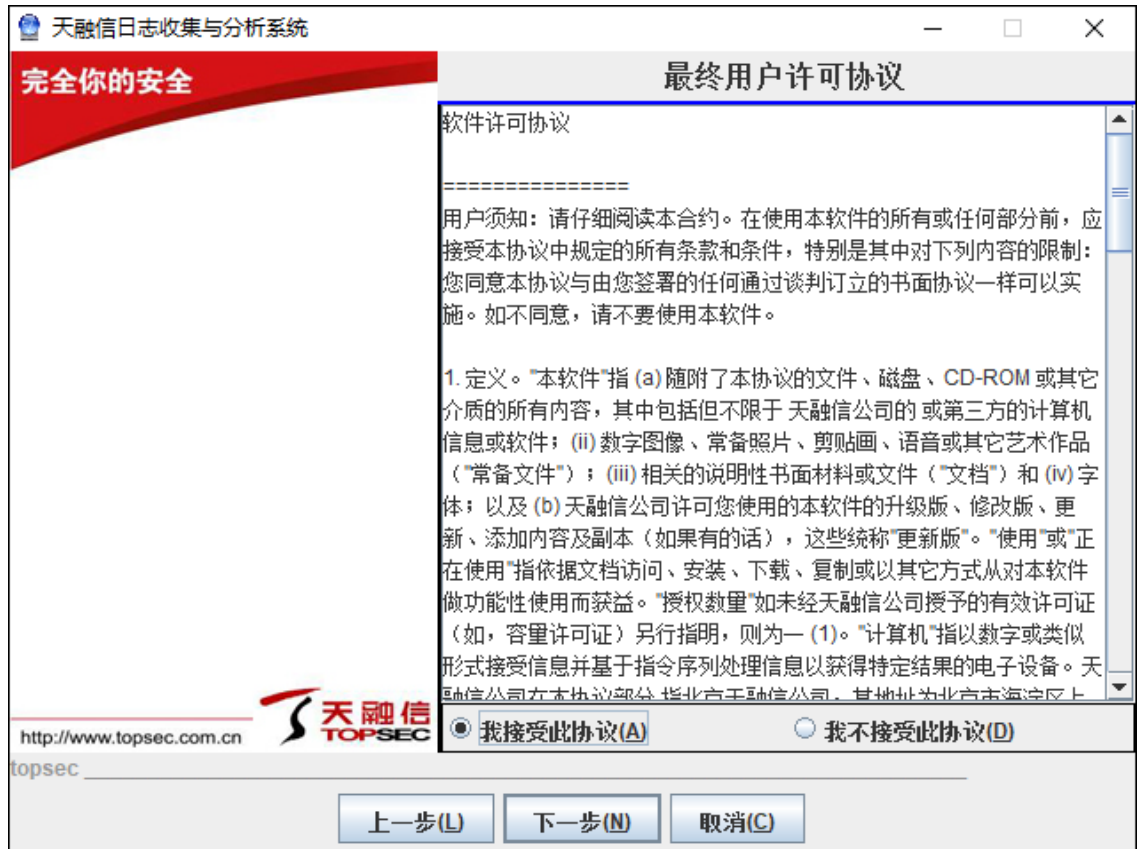
### 3.2.1.2.2 下级节点

安装 TA-L 服务器下级节点的具体步骤如下：

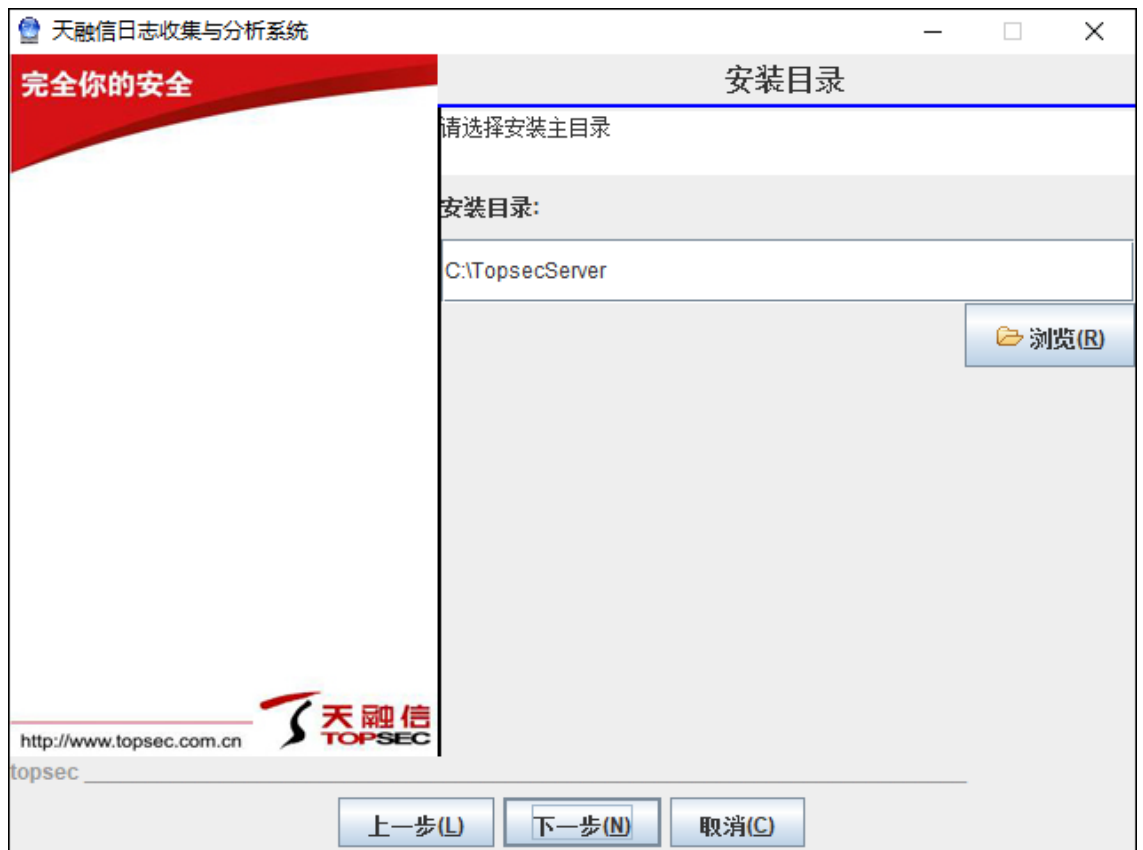
**步骤 1** 在安装光盘中，双击目录下的“setup.exe”，弹出如下图所示的窗口。



**步骤 2** 点击【下一步】按钮，接受最终用户许可协议，如下图所示。

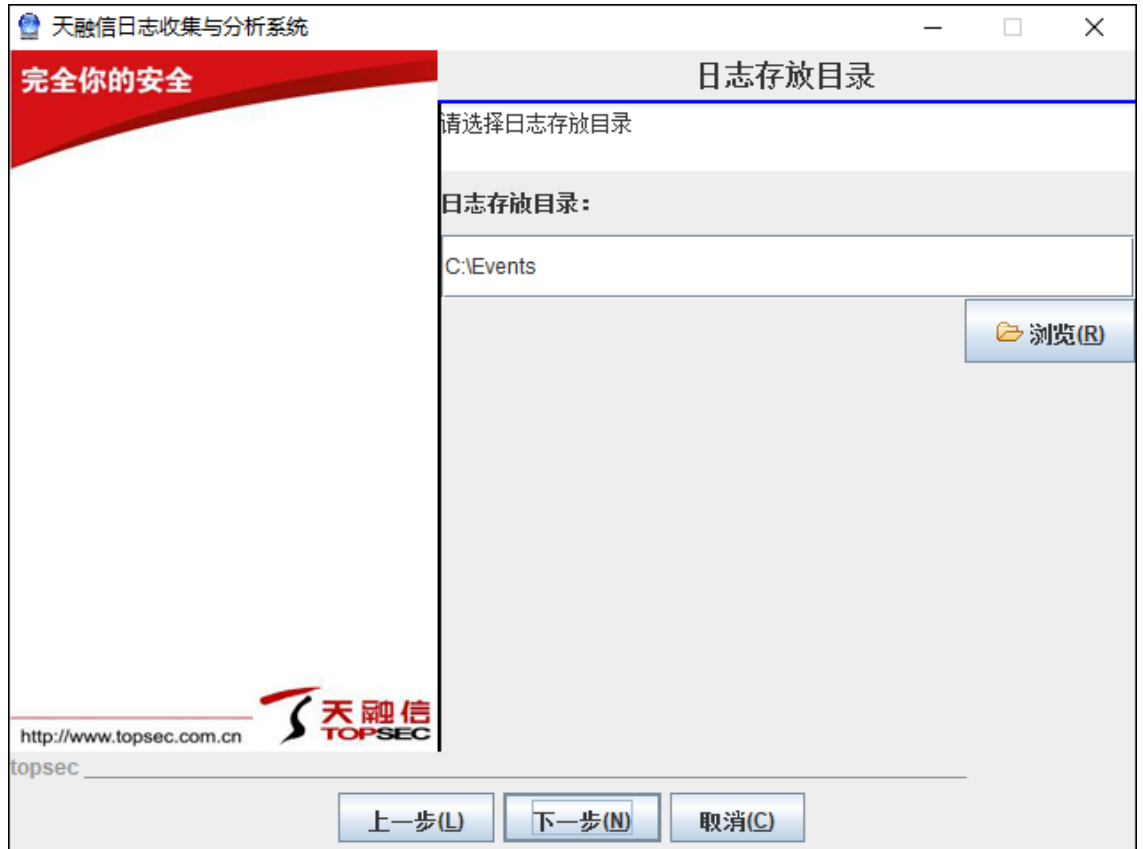


步骤 3 点击【下一步】按钮，设置安装目录。



默认的安装目录为：C:\TopsecServer，用户可以通过点击【浏览】按钮改变安装目录，建议将系统安装在足够空间的非系统盘中（注意：安装路径不支持中文和所有特殊字符）

**步骤 4** 点击【下一步】按钮，设置日志存放目录。



日志存放目录中将会存放大量的日志数据，建议选择较大的硬盘分区来存放日志。

**步骤 5** 点击【下一步】按钮，设置是否将 TA-L 安装为系统服务，如下图所示。



勾选“安装 Windows 服务”选项，输入计算机管理员帐号和密码并确认密码后，TA-L 服务器可以作为系统服务运行，服务名称为 TopAnalyzer。管理员可通过 **开始 > 程序 > 管理工具 > 服务** 对其进行启动和停止操作。

如果不勾选“安装 Windows 服务”选项，则不作为系统服务运行。安装完成后，可以通过 **开始 > 程序 > 天融信日志收集与分析系统 > 服务器** 来启动 TA-L 程序。

**步骤 6** 点击【下一步】按钮，选择安装的节点类型，选择下级节点，如下图所示。



TA-L 服务器支持两级部署模式，“管理节点”是指上级节点，只能部署一套，下级节点可以部署多套，输入上级节点 IP 地址和本级的 IP 地址。

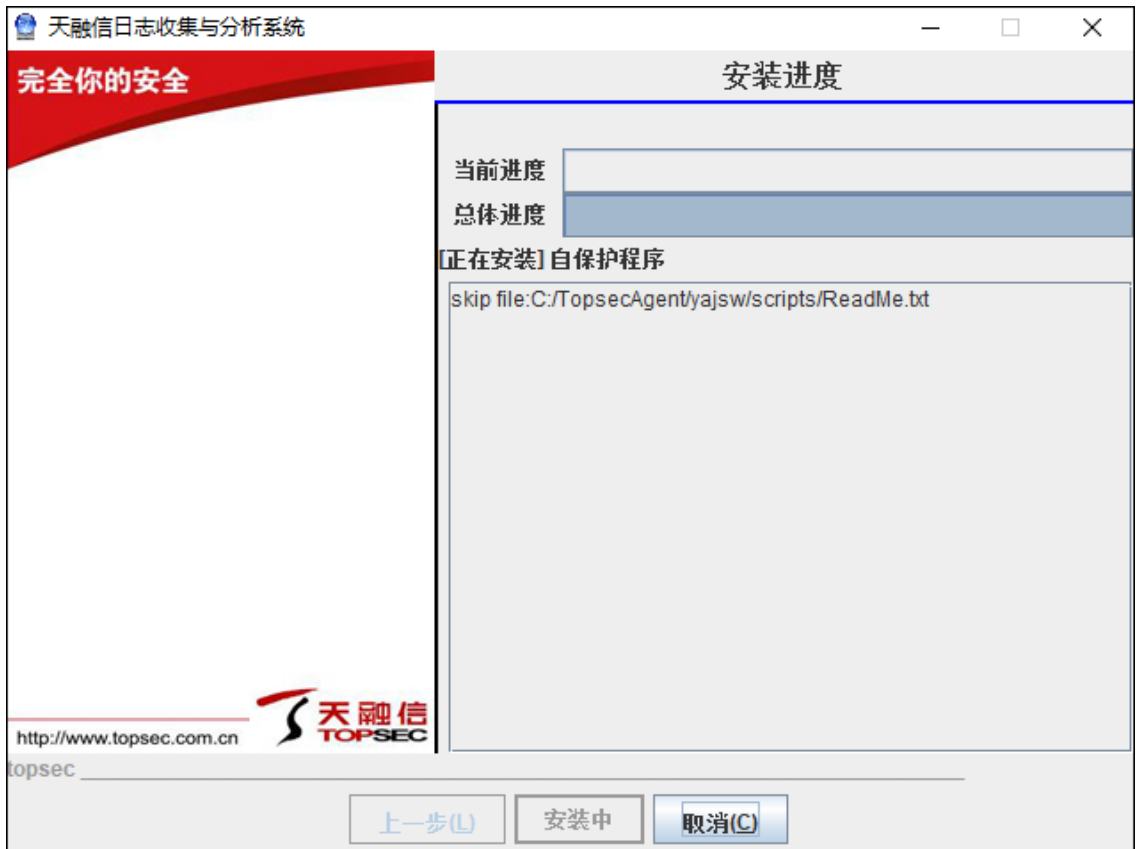
如勾选加密传输，则上下级之间的通信是加密传输，系统默认不加密，设置完成后点击【下一步】按钮即可。

**步骤 7** 点击【下一步】按钮，导入备份文件，如下图所示。



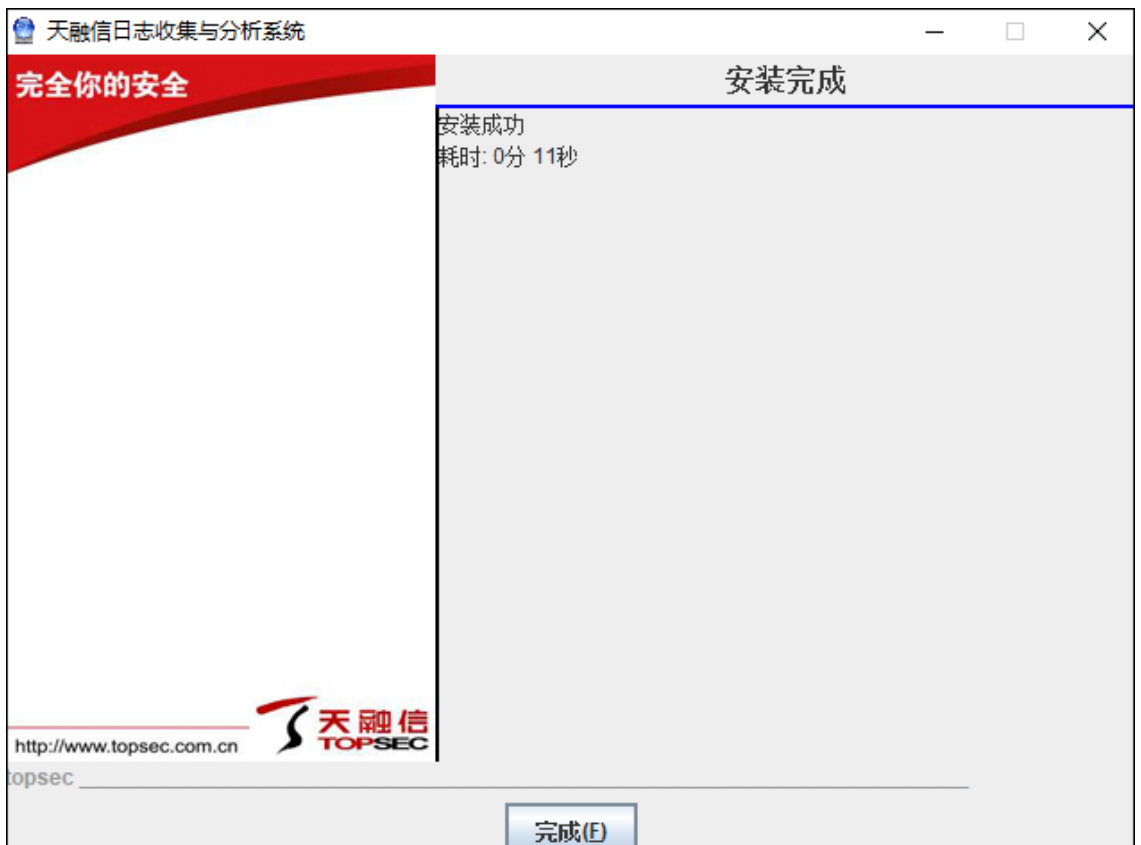
此步骤通常适用于重新安装系统时，管理员可以在此将事先导出的系统配置文件导入，以省略安装后的配置。当用户第一次安装时，可以忽略此步骤，直接点击【下一步】按钮即可。

**步骤 8** 点击【下一步】按钮，开始 TA-L 服务器的安装，如下图所示。



TA-L 系统的整个安装过程根据机器性能情况，持续时间不同，请用户耐心等待。

**步骤 9** 安装完成后，点击【完成】按钮退出安装程序，如下图所示。





---

至此，TA-L 服务器的安装完成。

## 3.2.2 安装收集代理

收集代理可负责代理所在网段的设备的日志收集（包括 syslog、snmp 等主动发日志的设备）和状态采集，一方面可分担 TA-L 服务器处理压力，另一方面当 TA-L 服务器无法管理的网段可通过安装代理进行管理。

### 3.2.2.1 安装环境

- 软件平台

操作系统：中文 windows 2003 (64 位) 服务器及以上版本

- 硬件平台

最低配置：

CPU：2 核以上处理器

内存：4G

硬盘：160G

推荐配置：

CPU：XEON 多核处理器

内存：4G 以上

硬盘：160G

**浏览器要求：**

ie9/10 版本

chrome 浏览器

火狐浏览器

ie 和火狐需要 flash 最新插件

### 3.2.2.2 安装代理

收集代理不能与 TA-L 服务器安装在同一台服务器上。

注意：代理安装包需要从 TA-L 服务器上下载，所以下载代理前，请先启动 TA-L 服务器，关于服务器的启动，请参见 [启动天融信日志收集与分析系统\(See 3.3\)](#)。

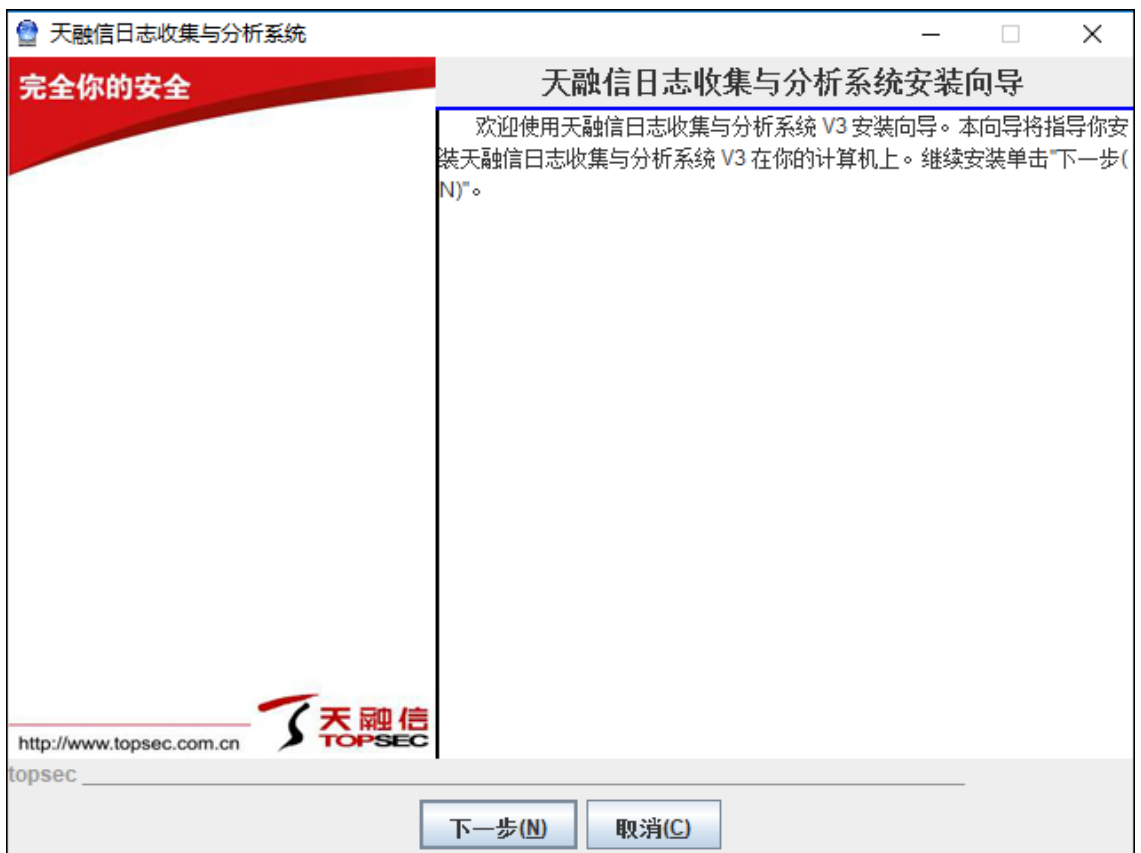
安装 TA-L 收集代理的具体步骤如下：

以操作管理员身份登录 TA-L 服务器，点击页面右上角的“”图标，在“产品信息”

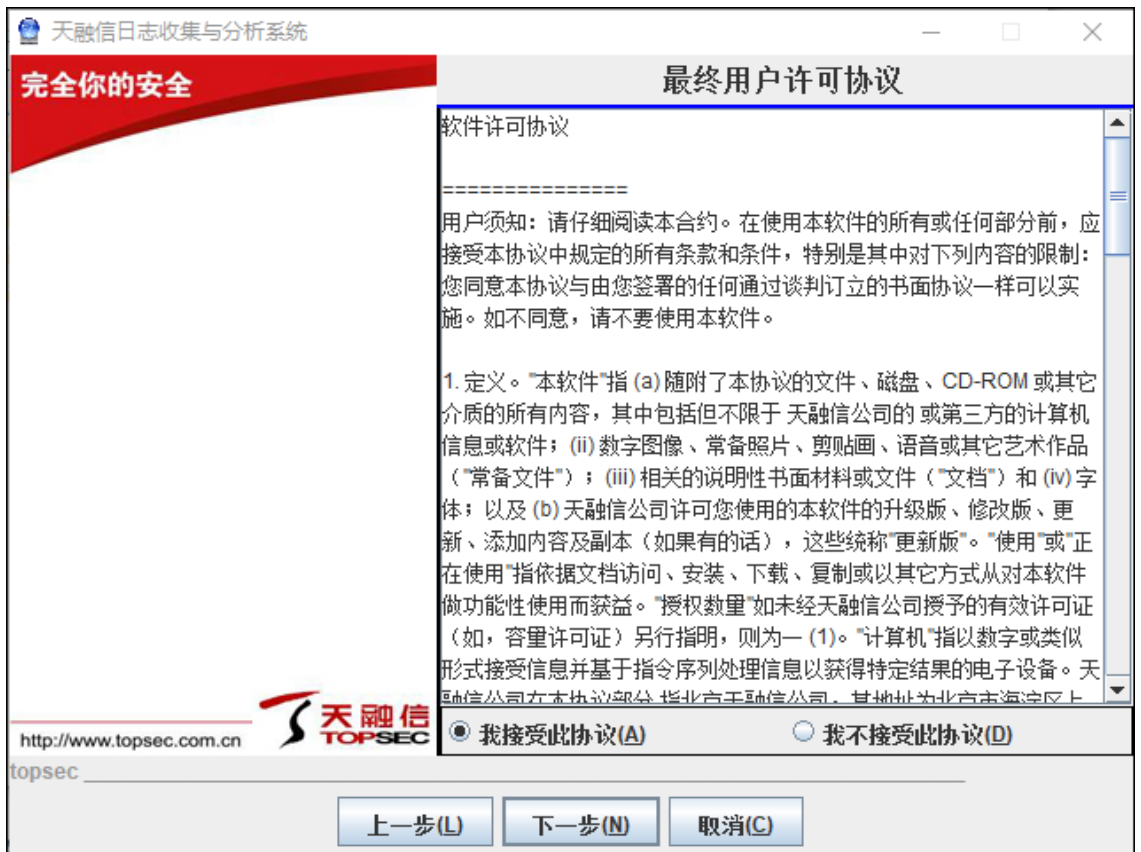
**步骤 1** 页面下载 Agent 安装包，如下图所示。



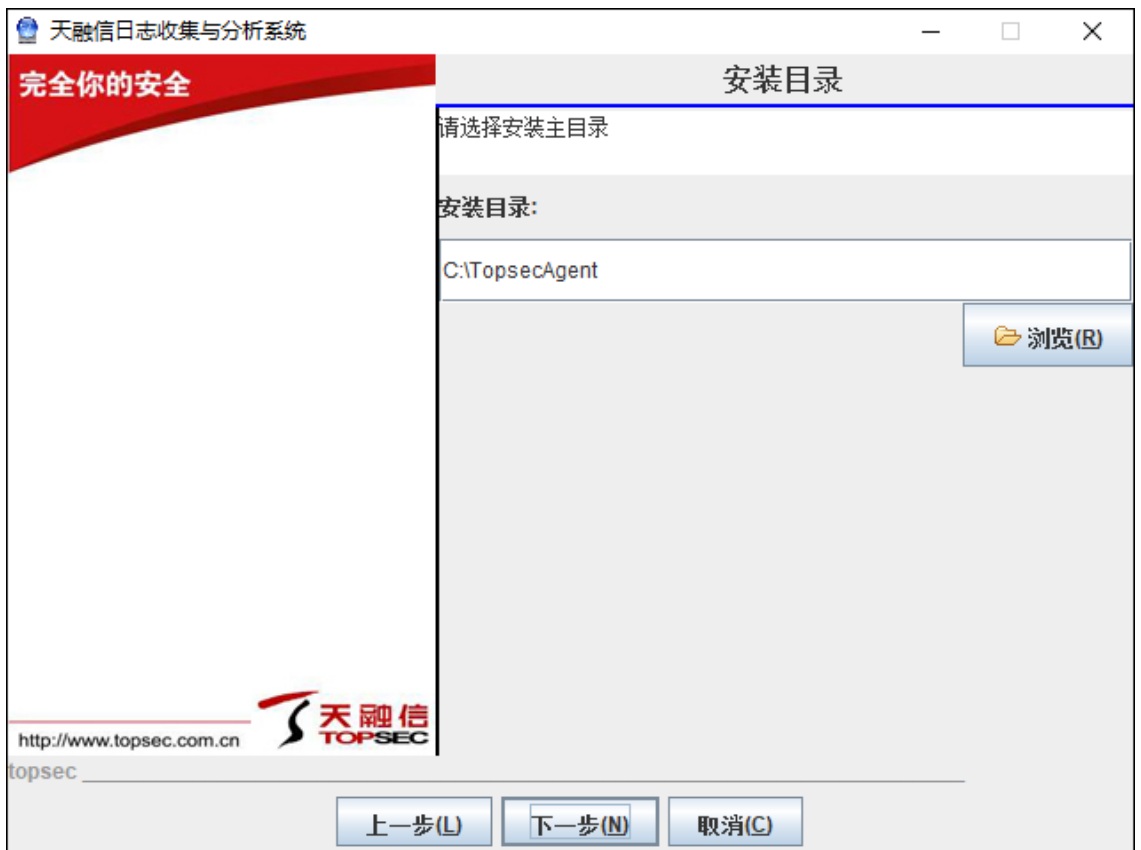
步骤 2 下载完成后，双击 Agent 安装包中的“setup.exe”，开始安装，弹出如下图所示的窗口。



步骤 3 点击【下一步】按钮，阅读并接受系统许可协议。



步骤 4 点击【下一步】按钮，设置安装目录，如下图所示。



默认的安装目录为：C:\TopsecAgent，用户可以通过点击【浏览】按钮改变安装目录，建议将系统安装在足够空间的非系统硬盘中。（安装目录不能包含所有特殊字符和中文）。

**步骤 5** 点击【下一步】按钮，设置 TA-L Agent 服务器的 IP 地址，如下图所示。



勾选“加密传输”，收集代理会将收集到的日志以加密方式传输至服务器。系统默认不加密。

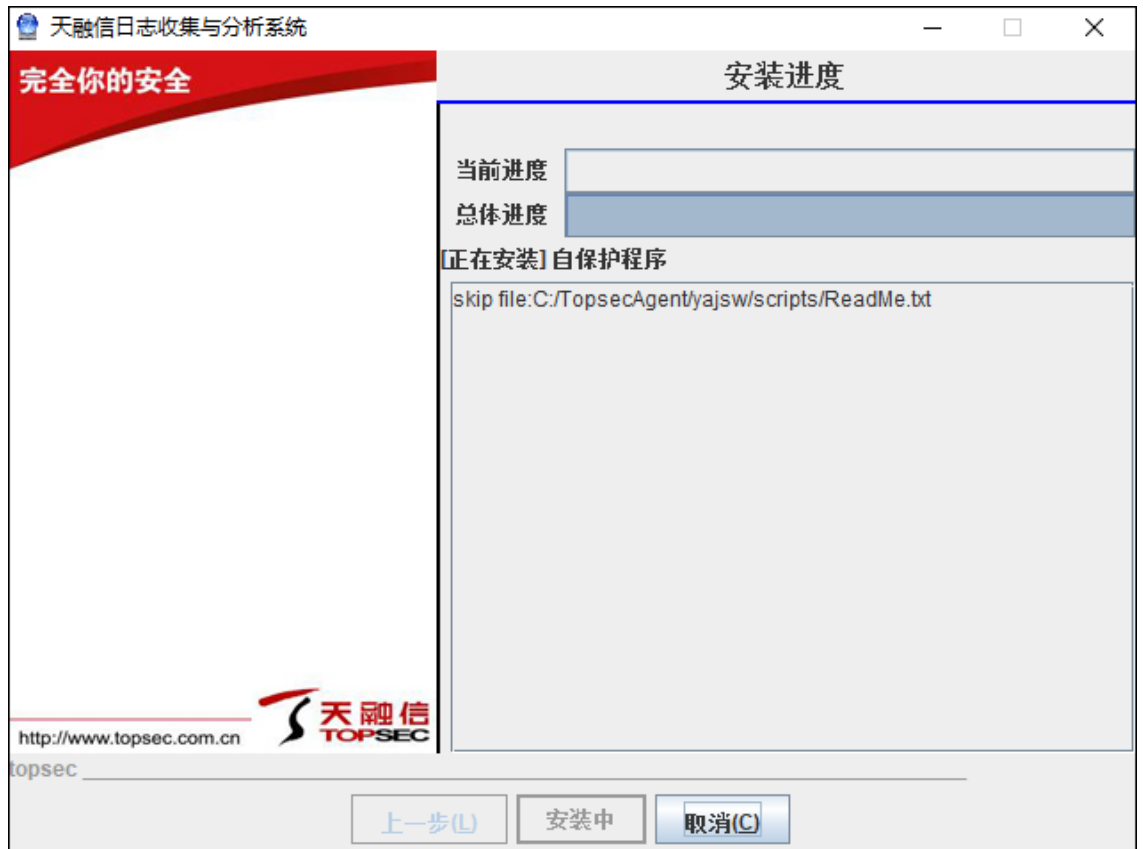
**步骤 6** 点击【下一步】按钮，设置是否将收集代理安装为系统服务，如下图所示。



勾选“安装 Windows 服务”选项，输入计算机管理员帐号、密码后，收集代理将作为系统服务运行，服务名称为 Topsec Agent。管理员可通过 **开始 > 程序 > 管理工具 > 服务** 对其进行启动和停止操作。此时的收集代理以后台程序方式运行。

如果不勾选“安装 Windows 服务”选项，则不作为系统服务运行。安装完成后，需要手工通过 **开始 > 程序 > 天融信日志收集与分析系统 > 收集代理** 来启动代理程序。

**步骤 7** 点击【下一步】按钮，开始收集代理的安装，如下图所示。



步骤 8 安装完成后，点击【完成】按钮退出安装程序，如下图所示。



---

至此，收集代理安装完成。

## 3.2.3 安装告警节点

用户在创建告警响应方式时，某些响应方式需要连接互联网或声卡，此时可在外网服务器或有声卡的主机上安装告警节点。

### 3.2.3.1 安装环境

#### ●软件平台

操作系统：中文 windows 2003 服务器及以上版本

#### ●硬件平台

最低配置：

CPU：2 核以上处理器

内存：4G

硬盘：160G

推荐配置：

CPU：XEON 多核处理器

内存：4G

硬盘：160G

### 3.2.3.2 安装告警程序

告警程序不能与 TA-L 服务器安装在同一台服务器上。

注意：告警程序安装包需要从 TA-L 服务器上下载，所以下载告警程序前，请先启动 TA-L 服务器，关于服务器的启动，请参见 [启动天融信日志收集与分析系统\(See 3.3\)](#)。

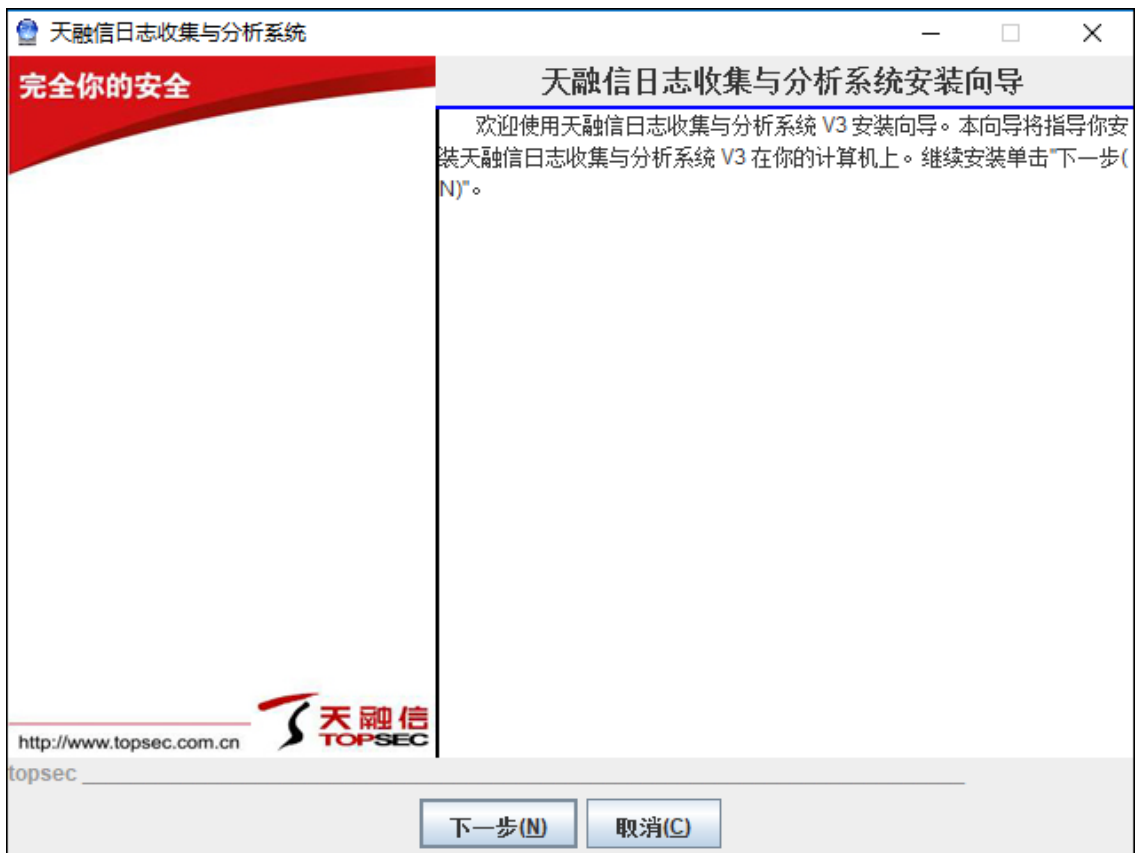
安装 TA-L 告警节点的具体步骤如下：

以操作管理员身份登录 TA-L 服务器，点击页面右上角的“”图标，在“产品信息”

**步骤 1** 页面下载告警程序安装包，如下图所示。

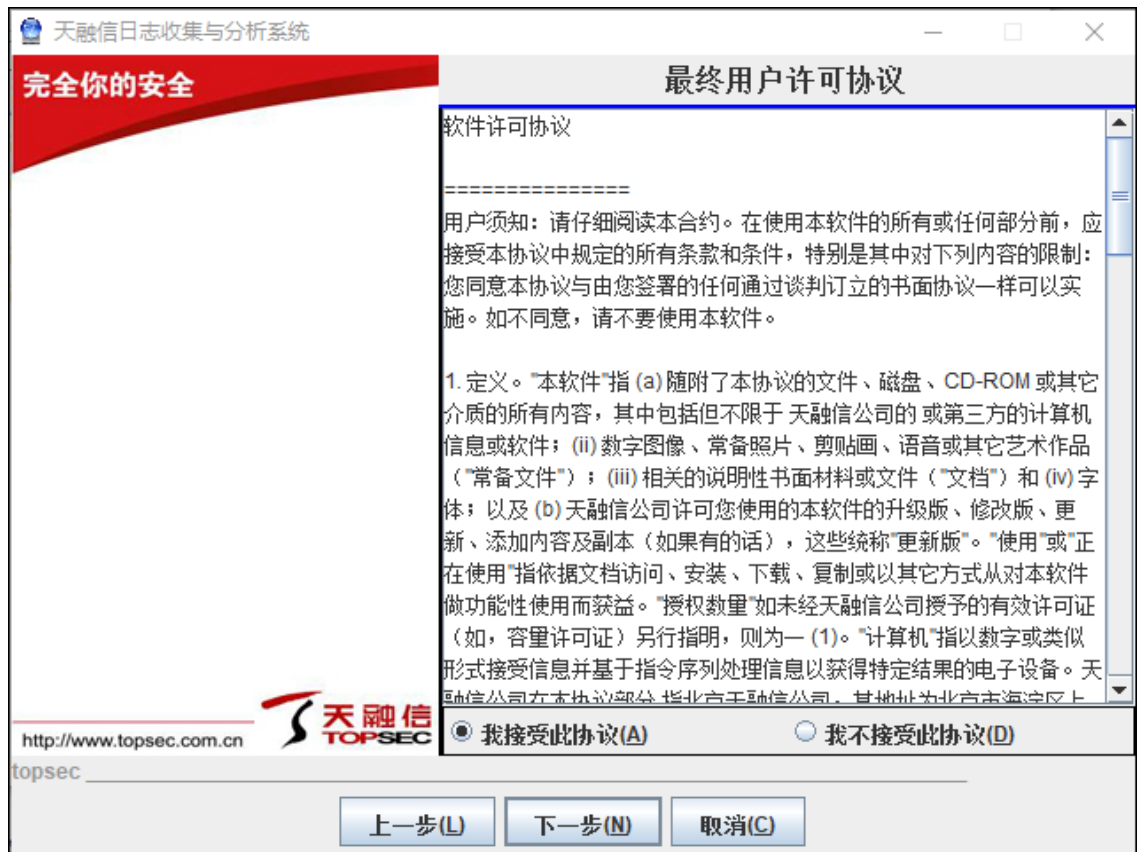


步骤 2 下载完成后，双击 Action 安装包中的“setup.exe”，开始安装，如下图所示。

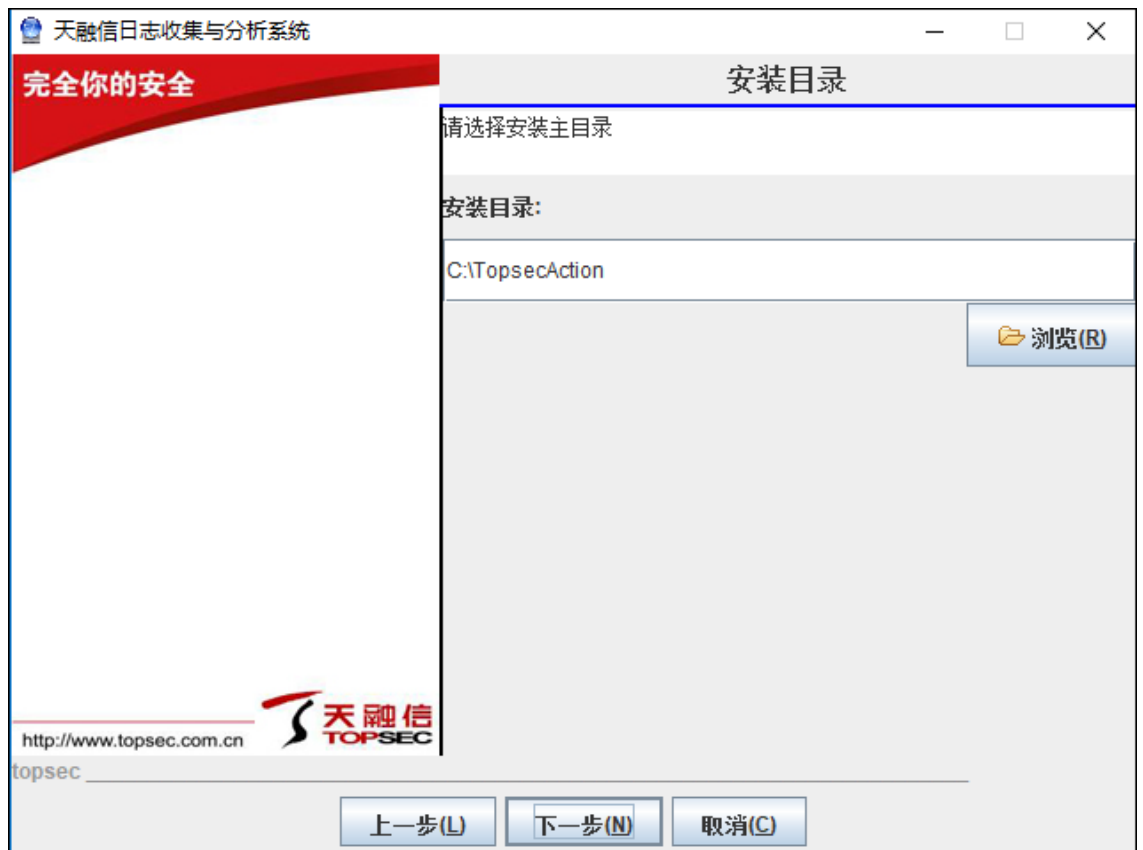


步骤 3 点击【下一步】按钮，阅读并接受系统许可协议，如下图所示。





步骤 4 点击【下一步】按钮，设置安装目录，如下图所示。



默认的安装目录为：C:\TopsecAction，用户可以通过点击【浏览】按钮改变安装目录，也可直接输入安装路径。对于不存在的安装目录，会提示是否自动创建。（安装目录不能包含所有特殊字符和所有特殊字符）。

**步骤 5** 点击【下一步】按钮，设置 TA-L 服务器的 IP 地址，如下图所示。



“上级服务器 IP”是指当前代理要连接的 TA-L 服务器的 IP 地址；“本级 IP”则是指当前告警节点的 IP 地址；“系统类型”是指安装告警节点的系统类型。

勾选“加密传输”，告警节点与服务器之间通信将会加密传输。系统默认不加密。

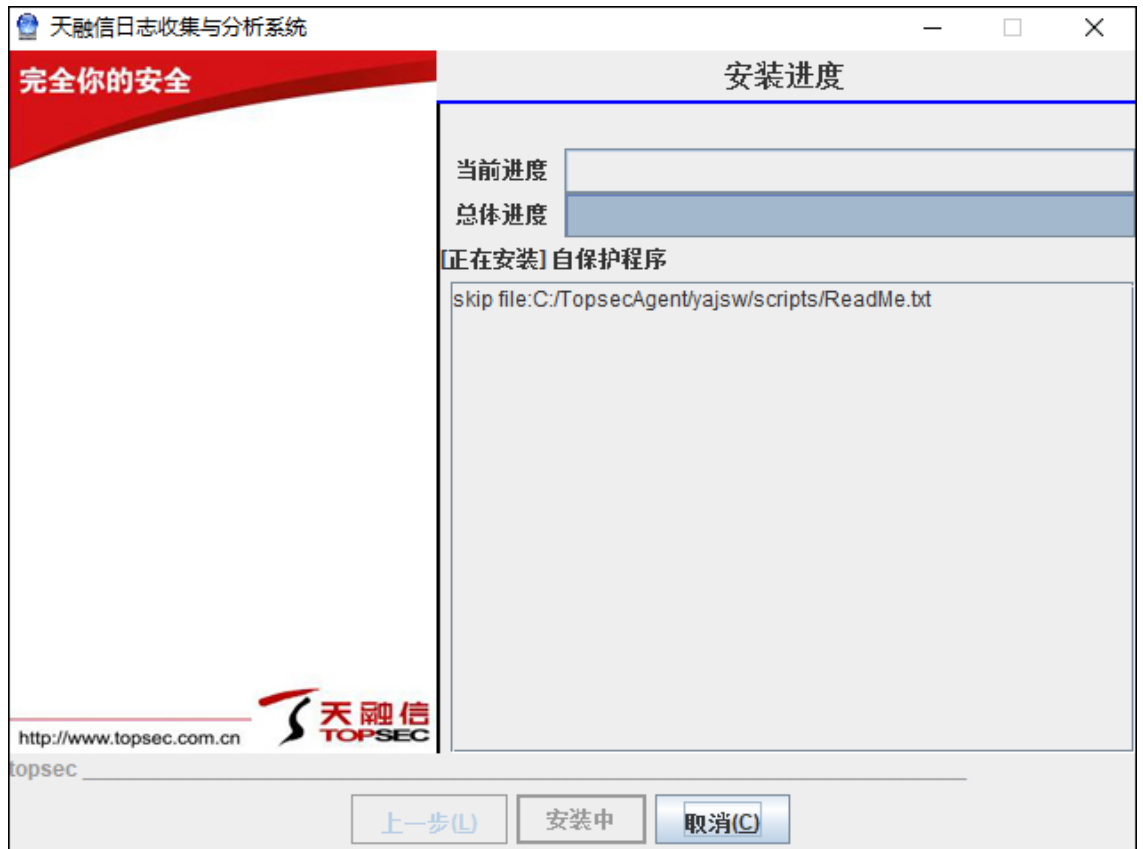
**步骤 6** 点击【下一步】按钮，设置是否将收集代理安装为系统服务，如下图所示。



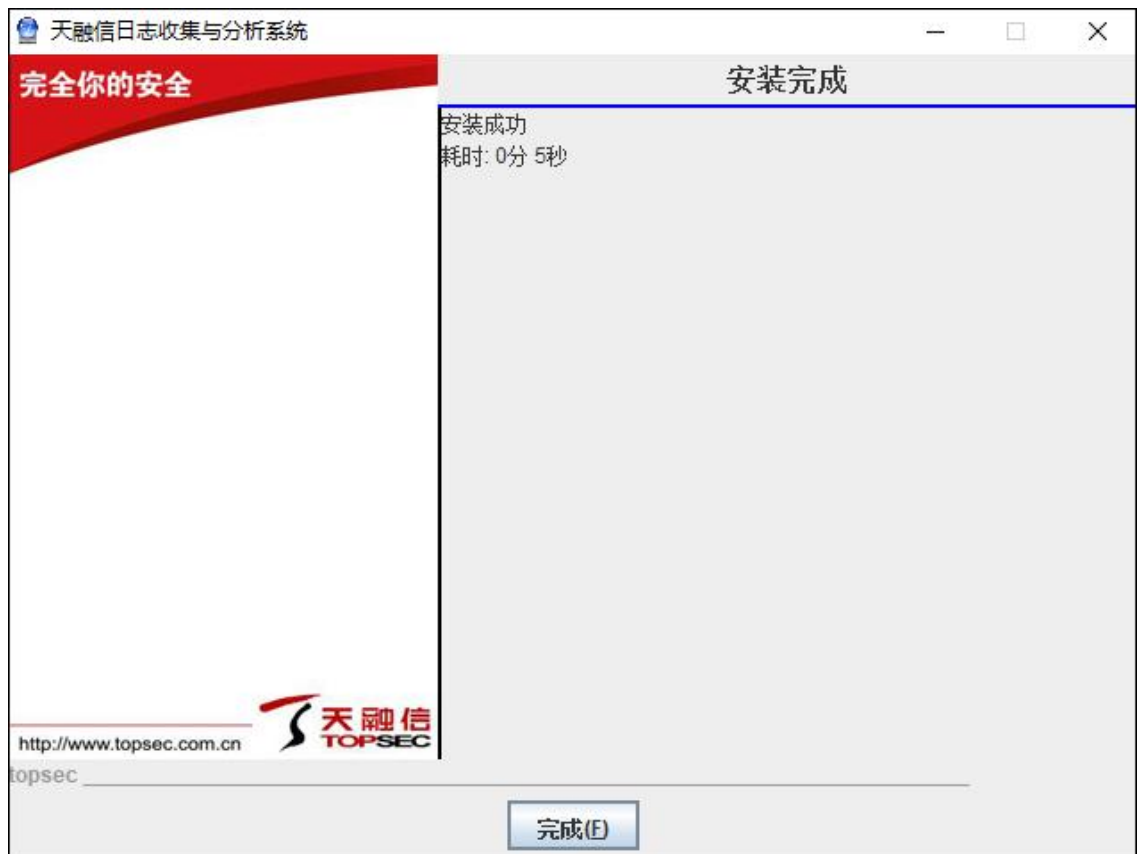
勾选“安装 Windows 服务”选项，输入计算机管理员帐号、密码后，告警程序将作为系统服务运行，服务名称为 Topsec Action。管理员可通过 **开始 > 所有程序 > 管理工具 > 服务** 对其进行启动和停止操作。此时的告警程序以后台程序方式运行。

如果不勾选“安装 Windows 服务”选项，则不作为系统服务运行。安装完成后，需要手工通过 TA-L Action 安装目录 \yajsw\bat 下的“start.bat”进行启动。

**步骤 7** 点击【下一步】按钮，开始告警程序的安装，如下图所示。



步骤 8 安装完成后，点击【完成】按钮退出安装程序，如下图所示。



---

至此，告警节点安装完成。

## 3.3 启动天融信日志收集与分析系统

TA-L 系统安装完成后，需要启动服务器才能开始使用。

TA-L 存在以下两种启动方式：

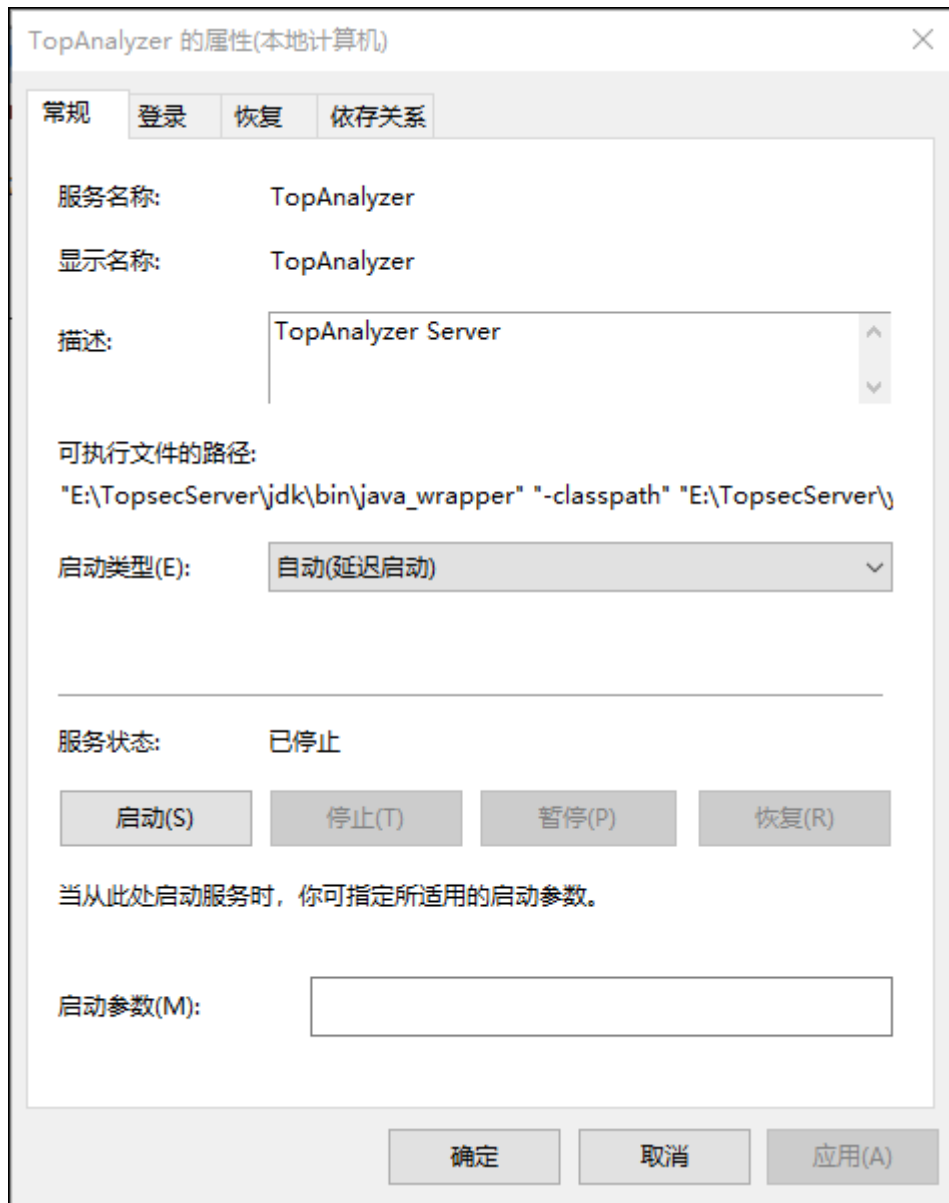
- [系统服务方式](#) (See 3.3.1)：TA-L 系统以系统服务的形式在后台运行。如果安装时勾选了“安装 Windows 服务”选项，方可以该种方式启动。
- [应用程序方式](#) (See 3.3.2)：TA-L 系统以应用程序方式在前台运行。当安装时未勾选“安装 Windows 服务”选项时，方可以该种方式启动。

### 3.3.1 系统服务启动方式

TA-L 系统以系统服务方式运行时，具体启动步骤如下：

#### 步骤 1 启动 TA-L 服务器服务

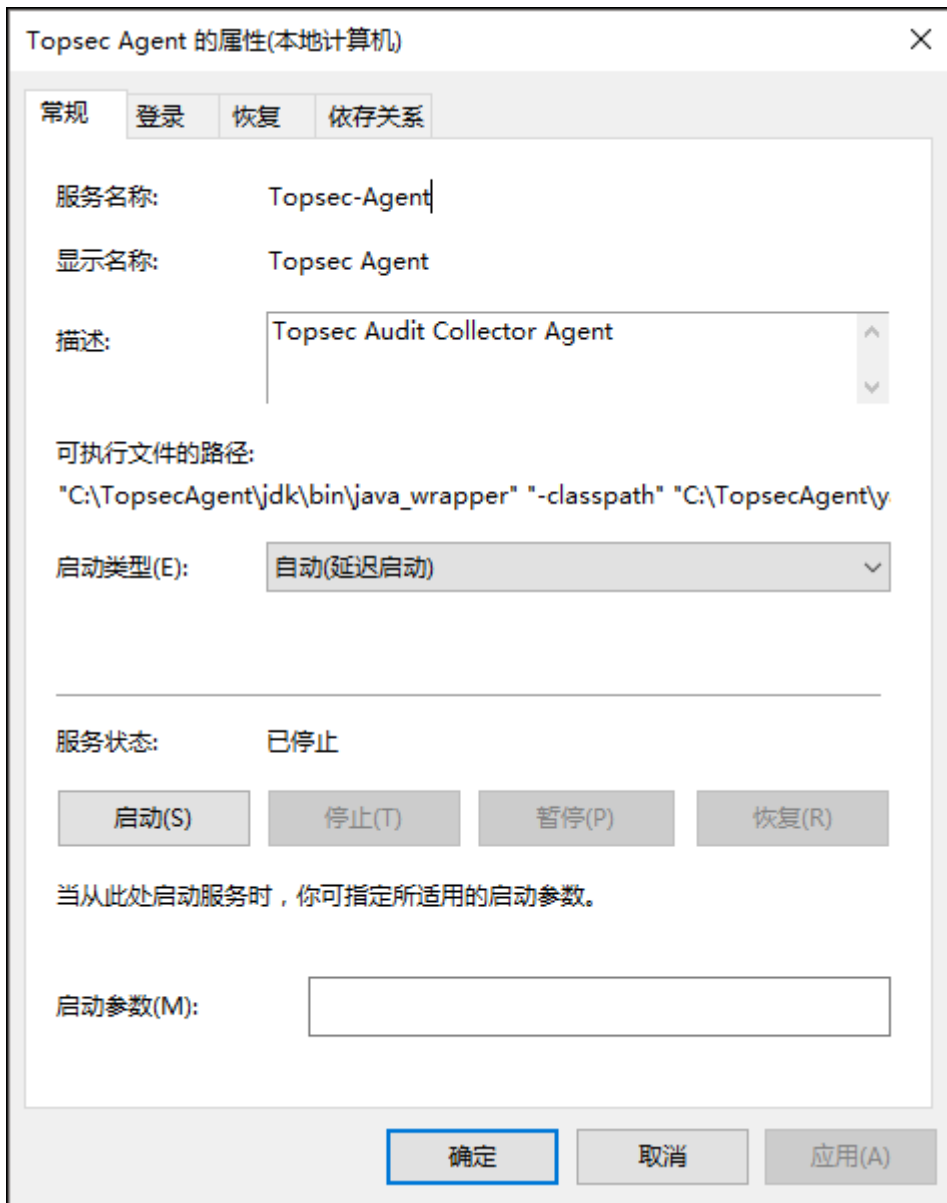
在 TA-L 服务器上，选择 **开始** > **程序** > **管理工具** > **服务**，启动 TopAnalyzer 服务，如下图所示。



点击【启动】按钮便可启动该服务。启动过程大概需要 1-2 分钟时间，请用户耐心等待。（请确保启动服务的帐号具有以服务启动的权限，如果启动失败请检查该项）

## 步骤 2 启动收集代理

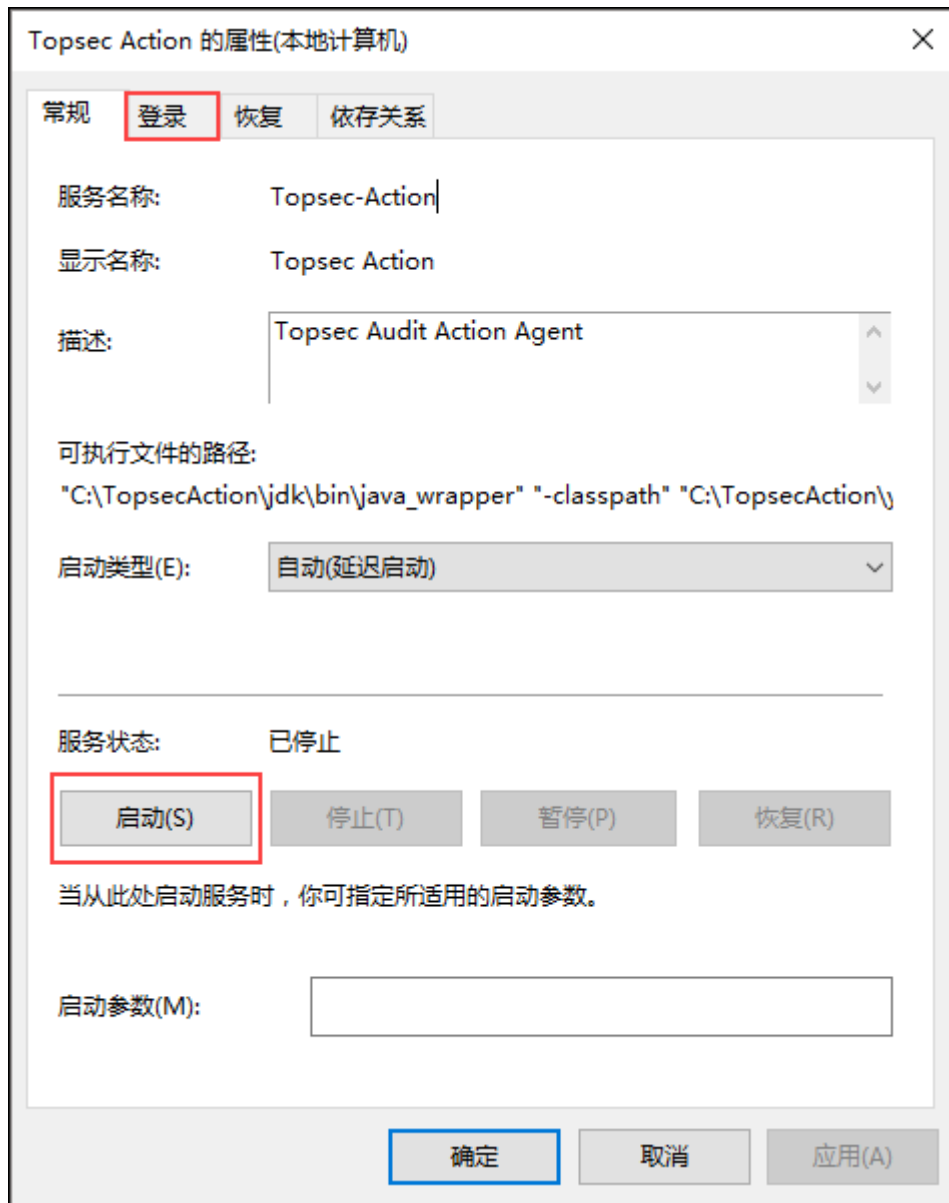
在收集代理服务器上，选择 **开始 > 程序 > 管理工具 > 服务**，启动 Topsec Agent 服务，如下图所示。



点击【启动】按钮便可启动该服务。启动过程大概需要 1 分钟时间，请用户耐心等待。

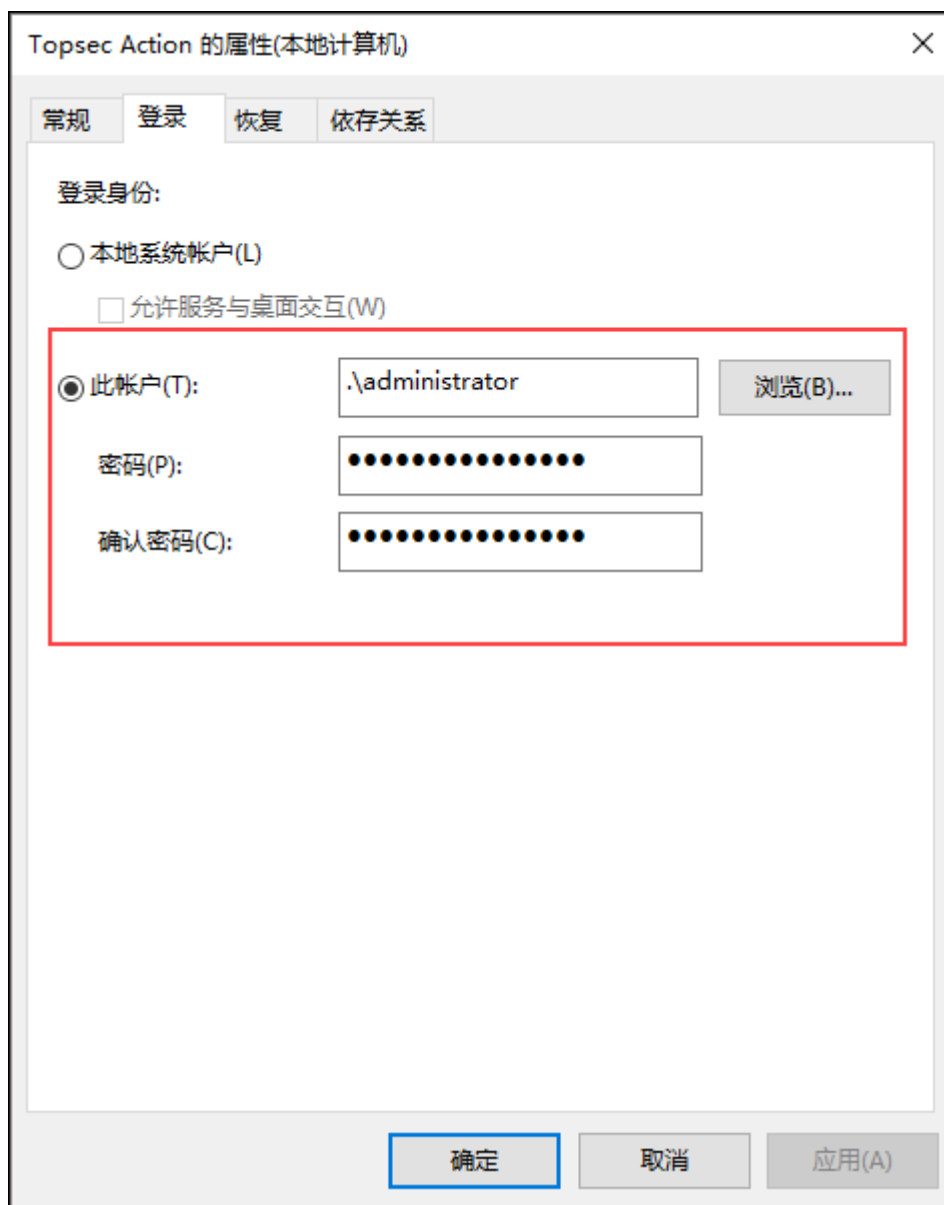
### 步骤 3 启动告警节点

在告警节点服务器上，选择 开始 > 所有程序 > 管理工具 > 服务，双击 Topsec Action 服务，弹出如下图的窗口。



选择“登录”页签，赋予当前操作系统用户（需是管理员）登录权限，如下图所示。





设置完成后，点击“常规”页签的【启动】按钮，便可启动该服务。

当需要关闭 TA-L 应用时，只需停止 TopAnalyzer、Topsec Agent、Topsec Action 服务即可。

### 3.3.2 应用程序启动方式

TA-L 系统以应用程序方式运行时，具体启动步骤如下：

在 TA-L 服务器上，选择 开始 > 程序 > 天融信日志收集与分析系统 > 服务器，启动  
步骤 1 TA-L 服务器程序，如下图所示。

```

服务器
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration AutoProtectedHandler
INFO 5032/0 Auditor 18-07-23 15:34:35 成功: 消息已发往内核
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [AutoProtectHandler main] - 关闭自保护!
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration JmsCollector
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration JmsCollector
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration FilterHandler
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration ProtocolMappingHandler
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration SyslogForwardHandler
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - setConfiguration EventDetectHandler
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - Initialize running configuration success!
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [NodeContainer main] - Start initialize components!
INFO 5032/0 Auditor 18-07-23 15:34:35 INFO [PoolingHandler main] - PoolingHandler buffer size: 4096
INFO 5032/0 Auditor 18-07-23 15:34:36 INFO [FailoverTransport ActiveMQ Task-1] - Successfully connected to nio://local
host:61616?wireFormat.maxInactivityDuration=300000&tcpNoDelay=true
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [FlexerHandler main] - FlexerHandler buffer size: 2048
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [JMSForwardHandler main] - JmsForwardHandler buffer size: 2048
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [AutoProtectHandler main] - initialize AutoProtectedHandler AutoProtectedHa
ndler
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [JmsEventCollector main] - JmsEventCollector buffer size: 2048
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [JmsEventCollector main] - JmsEventCollector buffer size: 2048
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [ArchiveUtils RepairArchive] - 修复 C:/Events/events/Esm_Topsec_SystemRunLo
g/127.0.0.1/2018/07/23/20180723143454171.dat
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [SyslogForwardHandler main] - SyslogForwardHandler buffer size: 2048
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [NodeContainer main] - Initialize components end!
INFO 5032/0 Auditor 18-07-23 15:34:37 INFO [NodeContainer main] - Start components!
INFO 5032/0 Auditor 18-07-23 15:34:38 INFO [EventCorrelationEngine main] - Start event correlation thread!
INFO 5032/0 Auditor 18-07-23 15:34:38 INFO [EventDetectHandler main] - EventDetectHandler is started!
INFO 5032/0 Auditor 18-07-23 15:34:38 INFO [NodeContainer main] - Start components end!
INFO 5032/0 Auditor 18-07-23 15:34:38 INFO [NodeContainer main] - node started!

```

当看到以上信息时，就可以登录服务器进行配置管理了。



◆当无法在开始菜单中找到程序时，也可通过 TA-L 服务器安装目录\yajsw\bat 下的“start.bat”进行启动。

步骤 2 在收集代理服务器上，选择 开始 > 程序 > 天融信日志收集与分析系统 > 收集代理，启动收集代理程序，如下图所示。

```

cmd CAWindows\system32\cmd.exe
INFO wrapper@Agent118-08-16 11:14:51: started process with pid 41980
INFO 41980-0@Agent118-08-16 11:14:53: [INFO] StandardFileSystemService - Using "ofs.tmp" as temporary files store.
INFO 41980-0@Agent118-08-16 11:14:57: Decrypt Warning!
INFO 41980-0@Agent118-08-16 11:14:57:ivcon Final block not properly padded
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize connection!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Connect connection
INFO 41980-0@Agent118-08-16 11:15:00: INFO [FailoverTransport ActiveMQ Task-1] - Successfully connected to tcp://172.17.62.13:61616?wireFormat.maxInactivityDuration=300000&tcpNo
Delay=true
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Start initialize channel!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize command channel 'CommandChannel'!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize command channel 'CommandChannel'!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize command channel 'KeepAliveChannel'!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize event channel 'EventChannel'!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize event channel 'AuditChannel'!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize channels success!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [AuditNodeContainer main] - Initialize communication end!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Start initialize components end!
INFO 41980-0@Agent118-08-16 11:15:00: INFO [NodeContainer main] - Initialize components env end!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - Initialize running configuration!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - Get configuration from superior!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - Register configuration to superior!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration FlexerHandler
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration 计划任务收集器
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration SyslogCollector
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration FlowCollector
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration ForwardEventHandler
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration 事件上传过滤器
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration AutoProtectHandler
INFO 41980-0@Agent118-08-16 11:15:01: INFO [AutoProtectHandler main] - 关闭自保护!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - setConfiguration SmpCollector
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - Initialize running configuration success!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [NodeContainer main] - Start initialize components!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [FlexerHandler main] - FlexerHandler buffer size: 2048
INFO 41980-0@Agent118-08-16 11:15:01: INFO [SchedulerCollector main] - SchedulerCollector initialize begin!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [SchedulerCollector main] - SchedulerCollector initialize end!
INFO 41980-0@Agent118-08-16 11:15:01: INFO [SyslogCollector main] - SyslogCollector buffer size: 1024
INFO 41980-0@Agent118-08-16 11:15:01: INFO [FlowCollector main] - FlowCollector buffer size: 2048
INFO 41980-0@Agent118-08-16 11:15:01: INFO [AutoProtectHandler main] - initialize AutoProtectHandler AutoProtectHandler
INFO 41980-0@Agent118-08-16 11:15:02: INFO [NodeContainer main] - Initialize components end!
INFO 41980-0@Agent118-08-16 11:15:02: INFO [NodeContainer main] - Start components!
INFO 41980-0@Agent118-08-16 11:15:02: INFO [SchedulerCollector main] - SchedulerCollector start begin!
INFO 41980-0@Agent118-08-16 11:15:02: INFO [SchedulerCollector main] - SchedulerCollector start end!
INFO 41980-0@Agent118-08-16 11:15:02: INFO [SyslogCollector main] - Syslog Server listening on port 514
INFO 41980-0@Agent118-08-16 11:15:02: INFO [FlowCollector main] - NetFlow Server listening on port 9991
INFO 41980-0@Agent118-08-16 11:15:03: INFO [SmpCollector main] - Smp Trap Agent listening on udp:0.0.0.0/162
INFO 41980-0@Agent118-08-16 11:15:03: INFO [SmpCollector main] - Smp Server listening on port 0.0.0.0/162
INFO 41980-0@Agent118-08-16 11:15:03: INFO [NodeContainer main] - Start components end!
INFO 41980-0@Agent118-08-16 11:15:03: INFO [NodeContainer main] - node started!
中文(简体) - 2345 五笔拼音输入法 半

```

当看到以上信息时，表示收集代理启动完成。



◇当无法在开始菜单中找到程序时，也可通过 TA-L Agent 安装目录\yajsw\bat 下的“start.bat”进行启动。

在告警节点服务器上，可通过 TA-L Action 安装目录\yajsw\bat 下的“start.bat”进行启动，启动告警程序，如下图所示。

**步骤 3**

```
C:\Windows\system32\cmd.exe
*
*      Beijing Topsec      *
*      Current Version: TA-L v3.3.10_Win      *
*
*****
[2018-08-16 11:17:15][NodeUpdateManager]setcl doesn't exist !!
INFO:41248/0>Action:18-08-16 11:17:15:started process with pid 41248
INFO:41248/0>Action:18-08-16 11:17:17:[INFO] StandardFileSystemManager - Using "ufs_tmp" as temporary files store.
INFO:41248/0>Action:18-08-16 11:17:21:Decrypt Warning!
INFO:41248/0>Action:18-08-16 11:17:21:Given final block not properly padded
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize connection!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Connect connection
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Start initialize channels!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize command channel 'CommandChannel'!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize command channel 'CommandChannel'!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize command channel 'KeepAliveChannel'!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize event channel 'ActionChannel'!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize event channel 'AuditChannel'!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize channels success!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [AuditNodeContainer main] - Initialize communication end!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Start initialize components env!
INFO:41248/0>Action:18-08-16 11:17:21:INFO [NodeContainer main] - Initialize components env end!
INFO:41248/0>Action:18-08-16 11:17:21:WARN [AuditNodeContainer main] - Message channel 'SUPERIOR_COMMAND' has not connected!
INFO:41248/0>Action:18-08-16 11:17:22:INFO [FailoverTransport ActiveMQ Task-1] - Successfully connected to tcp://192.168.75.52:61616?wireFormat.maxInactivityD
Delay=true
INFO:41248/0>Action:18-08-16 11:17:22:INFO [NodeContainer main] - Initialize running configuration!
INFO:41248/0>Action:18-08-16 11:17:22:INFO [NodeContainer main] - Get configuration from superior!
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - Regist configuration to superior!
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration con.topsec.tsa.node.component.handler.UMSGateActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration JmsCollector
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration SoundActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration ActionPoolingHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration MailActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration SmpActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration SmsActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration CommandActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration SoundShineActionHandler
INFO:41248/0>Action:18-08-16 11:17:23:INFO [NodeContainer main] - setConfiguration AutoProtectHandler
INFO:41248/0>Action:18-08-16 11:17:24:INFO [AutoProtectHandler main] - 关闭自保护!
INFO:41248/0>Action:18-08-16 11:17:24:INFO [NodeContainer main] - Initialize running configuration success!
INFO:41248/0>Action:18-08-16 11:17:24:INFO [NodeContainer main] - Start initialize components!
INFO:41248/0>Action:18-08-16 11:17:24:INFO [JmsEventCollector main] - JmsEventCollector buffer size: 2048
INFO:41248/0>Action:18-08-16 11:17:24:INFO [PoolingHandler main] - PoolingHandler buffer size: 4096
INFO:41248/0>Action:18-08-16 11:17:24:INFO [AutoProtectHandler main] - initialize AutoProtectHandler AutoProtectHandler
INFO:41248/0>Action:18-08-16 11:17:24:INFO [NodeContainer main] - Initialize components end!
INFO:41248/0>Action:18-08-16 11:17:24:INFO [NodeContainer main] - Start components!
INFO:41248/0>Action:18-08-16 11:17:24:INFO [NodeContainer main] - Start components end!
INFO:41248/0>Action:18-08-16 11:17:24:INFO [NodeContainer main] - node started!
中文(简体) - 2345 王牌拼音输入法 半
```

当看到以上信息时，表示告警程序启动完成。



◇多级部署时需要的网络条件：下级需要单项访问上级的 61616、61617、61618 端口，tcp 协议。

代理和告警节点需要单项访问服务器节点的 61616，61617 端口，tcp 协议。

### 3.3.3 登录 TA-L 系统

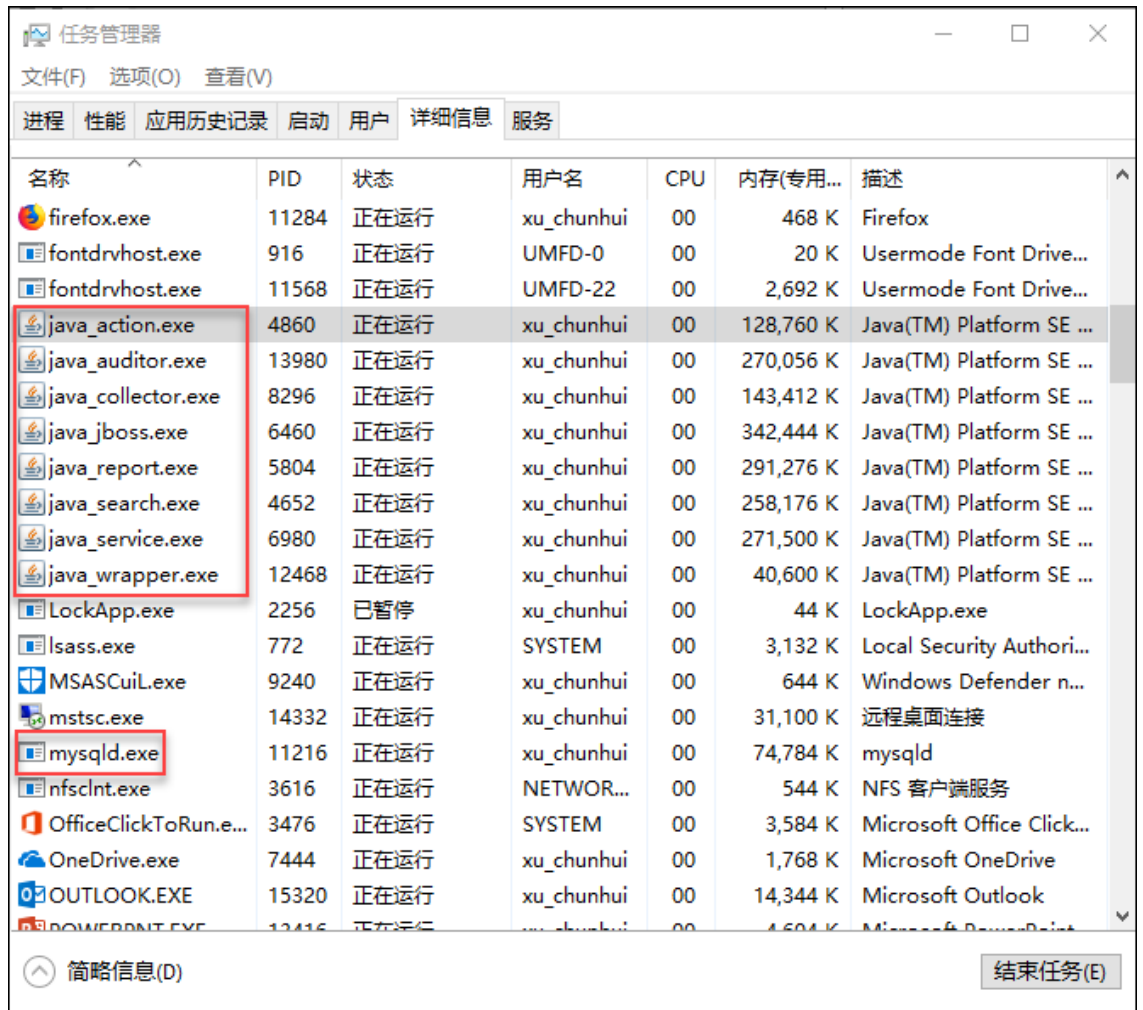
TA-L 服务器、收集代理启动完成后，便可通过 IE 浏览器登录 TA-L 系统。登录方式为：<https://TA-L 服务器 IP 地址>。例如，当 TA-L 服务器的 IP 地址为 192.168.25.220 时，则需在 IE 浏览器地址栏中输入：<https://192.168.25.220>，如下图所示。



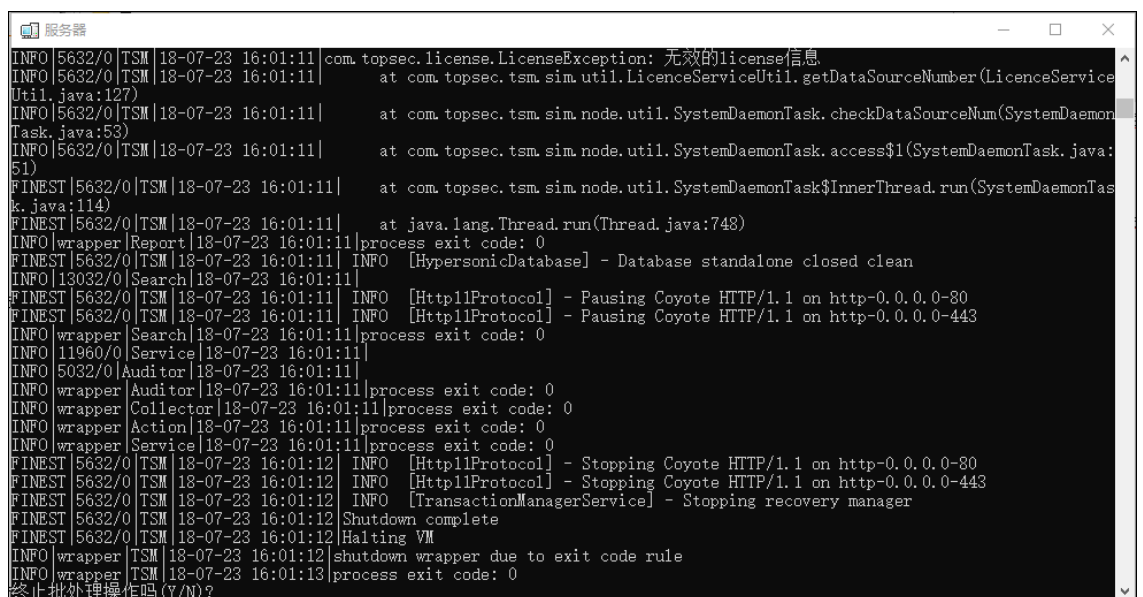
输入用户名、密码（默认三个用户，分别为：账户管理员 admin/talent123、操作管理员 operator/talent123、审计管理员 auditor/talent123）后，便可进行 TA-L 系统的配置和管理操作。具体使用方法请参考[操作管理员](#) (See 5.)、[审计管理员](#) (See 6.)、[账户管理员](#) (See 7.) 的相关内容。

## 3.4 关闭天融信日志收集与分析系统

TA-L 服务器在启动的模式下，停止程序需要在服务列表中找到相应的服务点击停止，为了确保进程都退出，需要在任务管理器的进程列表中，把 java 开头的进程和 mysqld 进程都结束，如下图所示。



需要特别注意的是，只有服务器端需要检查 mysql 进程，代理和告警节点没有 mysql。命令行窗口启动的模式下，停止程序需要同时按下 Ctrl+C 键（并根据提示信息输入“Y”，切勿直接关掉命令行窗口）如下图所示。



---

## 3.5 卸载天融信日志收集与分析系统

天融信日志收集与分析系统（TA-L）是天融信公司推出的绿色软件之一。安装过程中，可由用户决定是否改写系统注册表项，即是否勾选“安装 Windows 服务”选项。

当没有选择“安装 Windows 服务”选项时，其卸载简单，只需删除相应的安装目录和程序菜单

- 即可。

当选择“安装 Windows 服务”选项时，首先分别在服务器、代理、告警节点的安装目录 \yajsw\bat 下面运行“uninstallService”来删除对应的服务，然后再删除对应的安装目录和

- 程序菜单。

具体卸载过程及卸载中遇到的问题，可咨询天融信公司的技术支持人员。

## 4. 初次使用系统

本部分为初次使用天融信日志收集与分析系统的用户介绍如何登录系统，以及介绍系统三种用户。相关内容主要包括：

- [系统登录](#) (See 4.1)，介绍如何通过默认帐户登录系统。
- [系统用户](#) (See 4.2)，介绍管理系统的三种用户。

### 4.1 系统登录

用户在登录系统前应首先在网络中部署和安装天融信日志收集与分析系统服务器，安装并启动成功后，才能正常登录和管理系统。天融信日志收集与分析系统的安装请参见 [安装](#) (See 3.)。

登录系统的具体方法为：

管理员可以通过 HTTPS 协议以 WEB 访问的方式对天融信日志收集与分析系统进行远程管理。在访问时，管理员需要在管理主机的浏览器地址栏中输入系统服务器的管理 URL，

**步骤 1** 例如：<https://192.168.73.26>，进入如下的登录页面。



对应系统的三类管理员角色，系统预置了三个管理员包括：审计管理员 auditor、操作管理员 operator 和帐户管理员 admin（密码均为 talent123），初次登录系统时可使用这三个账号进行相应权限的操作。

**步骤 2** 点击登录页面的“更改密码”链接，可以修改管理员的登录密码。



**步骤 3** 另外，管理员第一次登录系统时会强制修改密码，如下图所示。



更改密码

第一次登录, 必须修改密码!

用户名 11111 ✓

原密码 密码

新密码 密码

确认密码 确认密码

提交更改 跳转到登录页面

天融信 TOPSEC

输入新密码后, 点击【提交更改】按钮, 便可完成密码的修改。修改密码后, 系统会自动跳转至登录页面, 此时需要管理员利用新密码重新登录系统。

## 4.2 系统用户

天融信日志收集与分析系统依据三权分立的设计原则将系统用户分为以下三个类型, 不同类型的用户对系统拥有不同的管理权限。

- [帐户管理员](#) (See 7.): 具有对系统用户账户进行管理的权限, 权限功能模块包括主页和用户。
- [操作管理员](#) (See 5.): 具有对系统 Web 界面进行管理和配置的权限, 权限功能模块包括主页、日志、报表、告警、日志源、知识库和配置。
- [审计管理员](#) (See 6.): 具有查看系统审计日志和审计报表的权限, 权限功能模块包括: 主页、日志和报表。

## 5. 操作管理员

操作管理员包括系统预置管理员 (账户为: operator/talent123) 和自定义管理员, 拥有 [主页](#) (See 5.1)、[日志](#) (See 5.2)、[报表](#) (See 5.3)、[告警](#) (See 5.4)、[日志源](#) (See 5.5)、[知识库](#) (See 5.6) 和 [配置](#) (See 5.7) 功能模块的管理权限。系统预置操作管理员和自定义的操作管理员功能权限稍有差异, 可查看的功能项有所不同, 具体以登录界面为准。



## 5.1 主页

天融信日志收集与分析系统作为管理节点时，主页可以展示总览和本级节点的各类统计情况；作为下级节点时，主页只可展示本级节点的各类统计情况，用户在主页页面可以分别查看。天融信日志收集与分析系统的节点类型在安装 TA-L 服务器时配置，安装过程请参见 [安装 TA-L 服务器](#) (See 3.2.1)。

### 查看总览

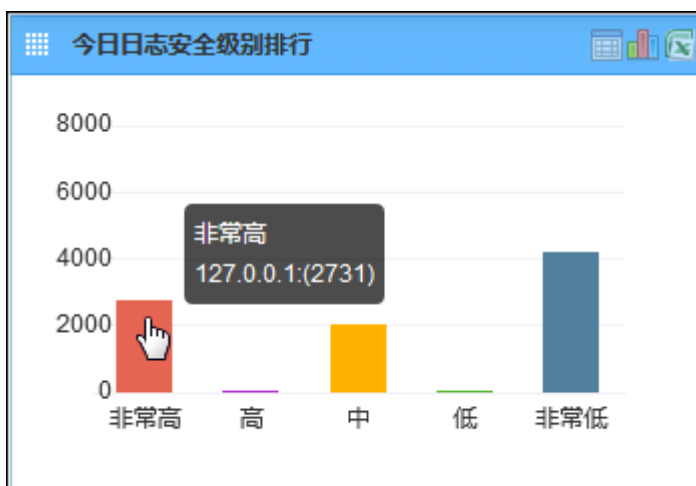
登录后选择 **主页** > **总览**（默认登录后的首页面），界面显示所有节点的各类统计图表和实时数据列表，包括今日日志安全级别排行、今日告警安全级别排行、系统拓扑图、日志地址区域分布图、日志总量统计、今日最新告警 Top10 的情况。如下图所示。



首页展示了以下几个方面内容：

- 今日日志安全级别排行。

在“今日日志安全级别排行”区域，显示系统中所有设备今日产生的日志安全级别统计情况，并以柱形图的形式展示各个安全级别的日志数量。将管理主机的鼠标移动至柱形图上的相应位置，系统将会显示该日志的安全级别名称、日志数量以及产生日志的节点 IP 地址。如下图所示。



点击相应位置则以该安全级别名称为查询条件跳转到“日志查询”页面。关于日志查询具体请参见 [日志查询](#) (See 5.2.3)。

- 今日告警安全级别排行

在“今日告警安全级别排行”区域，显示系统中所有设备今日产生的告警安全级别统计情况，并以柱形图的形式展示各个安全级别的告警数量。将管理主机的鼠标移动至柱形图上的相应位置，系统将会显示该告警的安全级别名称、告警数量以及产生告警的节点 IP 地址。如下图所示。



点击相应位置则以该安全级别名称为查询条件跳转到“告警查询”页面。关于告警查询具体请参见 [告警查询](#) (See 5.4.3)。

- 日志的源地址或目的地址区域分布图

该区域分布图上以闪烁圆圈的形式标出了该日志的源地址或者目的地址所属的区域，同时以不同的颜色标出了日志数量的不同（颜色越深表示日志数量越多）。用户可以以不同的视角查看今日数据分布情况，包括全国数据分布、全球数据分布。

(1) 全国数据分布。激活“全国数据分布”页签，如下图所示。



鼠标滑动至某区域，系统会显示该区域产生日志的源地址或者目的地址数量。点击某区域，可查看该区域产生日志的源地址或目的地址在各市、县的分布情况。点击某个闪烁的圆圈，系统会弹出新的页签进入日志查询页面，并且自动过滤出源地址或目的地址为当前区域的日志，用户可查看相应的日志详情。关于日志查询操作具体请参见 [日志查询](#) (See 5.2.3)。

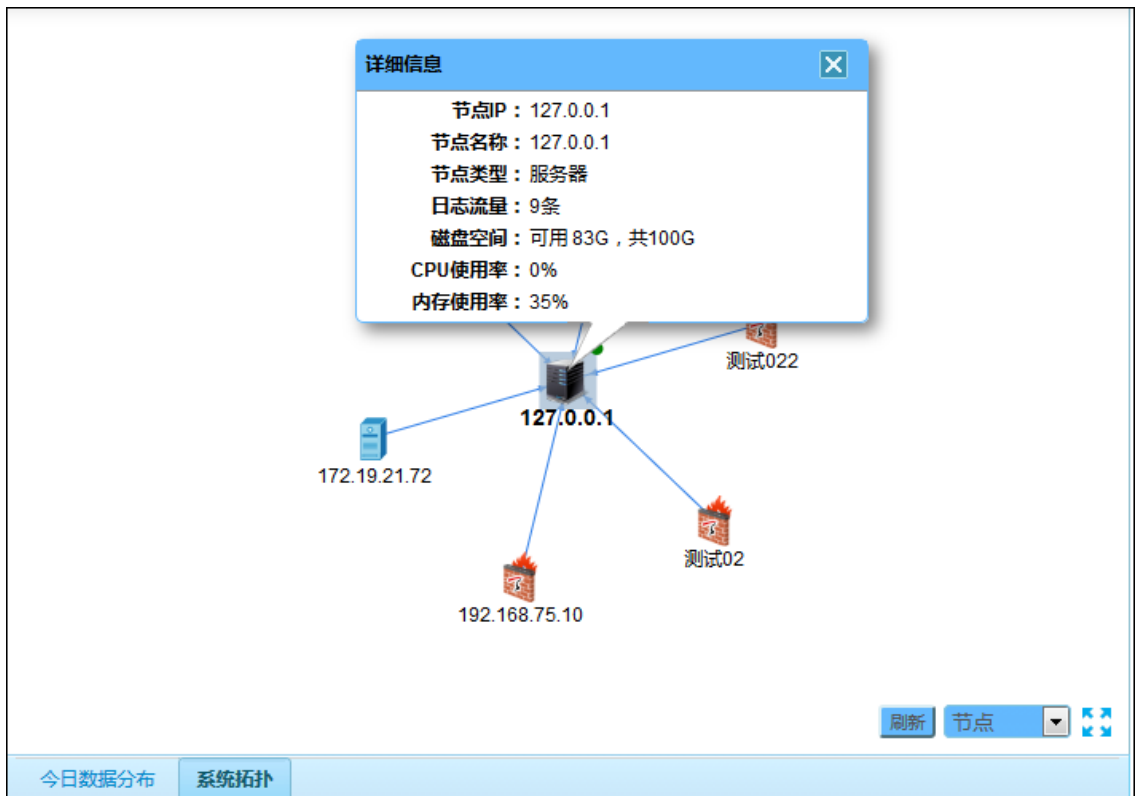
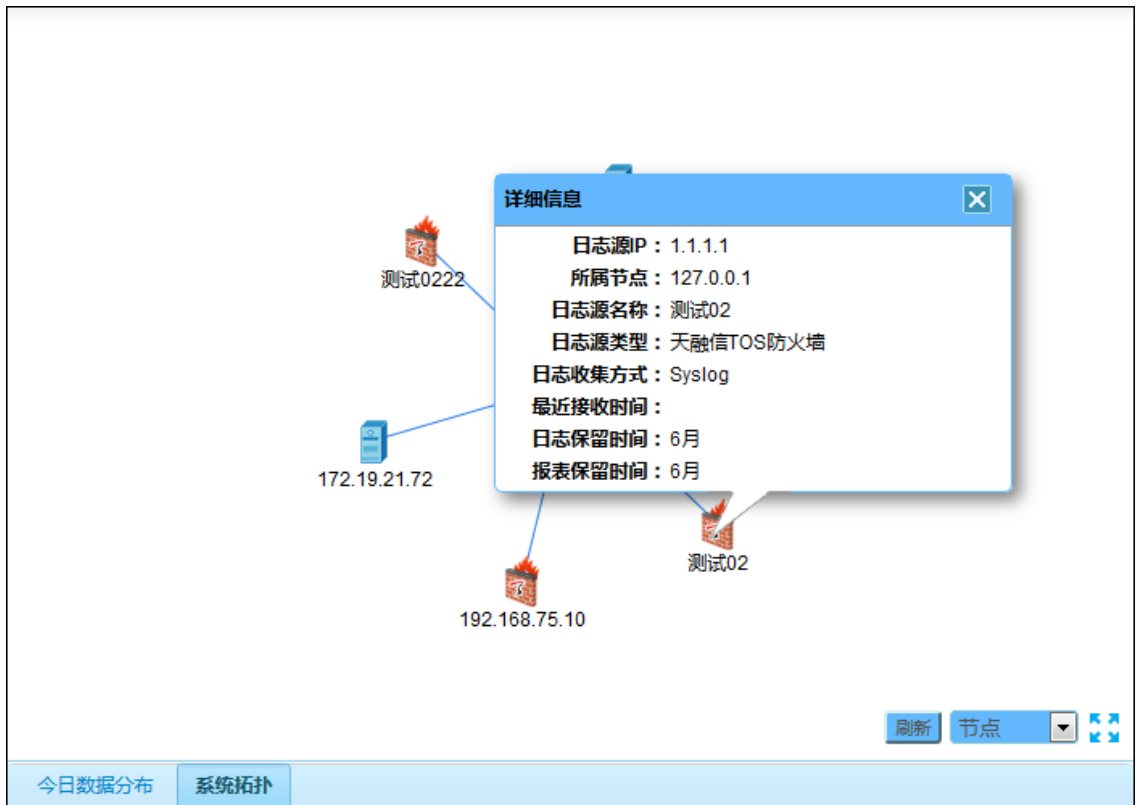
(2) 全球数据分布，激活“全球数据分布”页签，如下图所示。



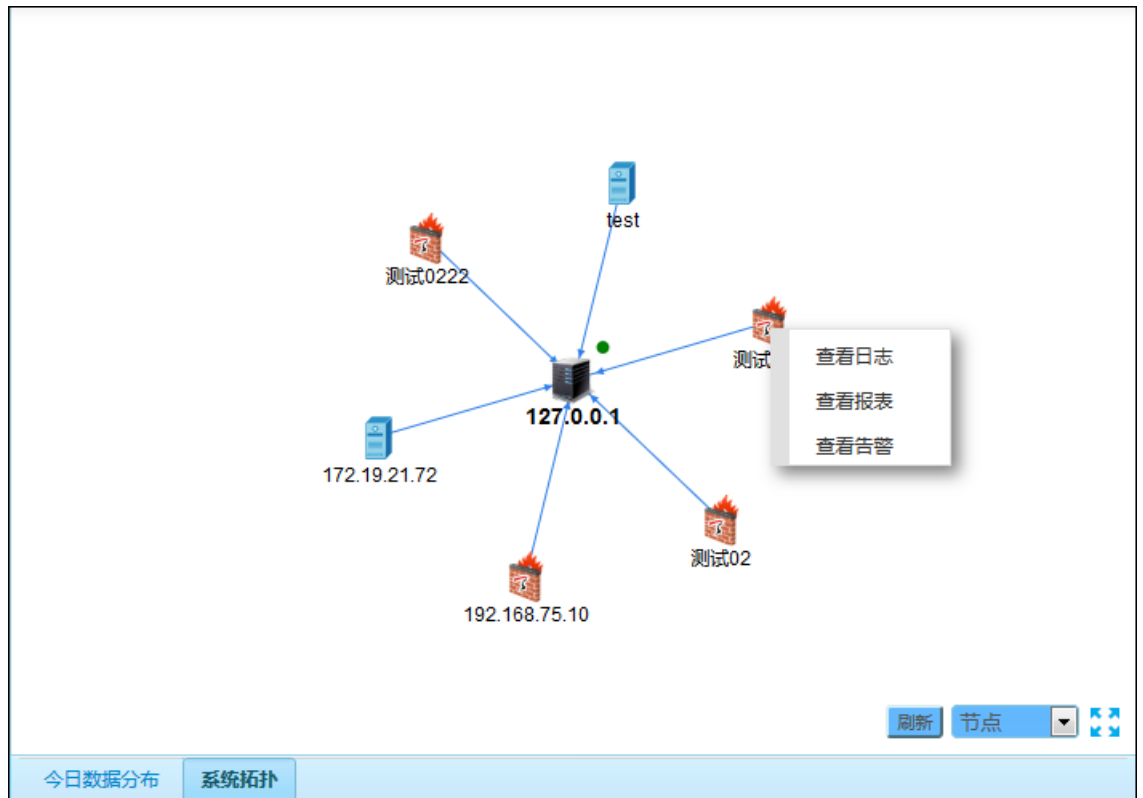
查看详情操作类似全国数据分布，此处不再赘述。


- 系统拓扑。

(1) 激活“系统拓扑”页签，可以看到管理员设置的默认的拓扑图。点击某个监视对象时，系统会弹出该监视对象详细信息的提示框，如果该监视对象是日志源，则包括日志源 IP、所属节点、日志源名称、日志源类型、日志收集方式、最近接收时间、日志保留时间以及报表保留时间；如果该监视对象是节点，则包括节点 IP、节点名称、节点类型、日志流量、磁盘空间、CPU 使用率以及内存使用率。如下图所示。

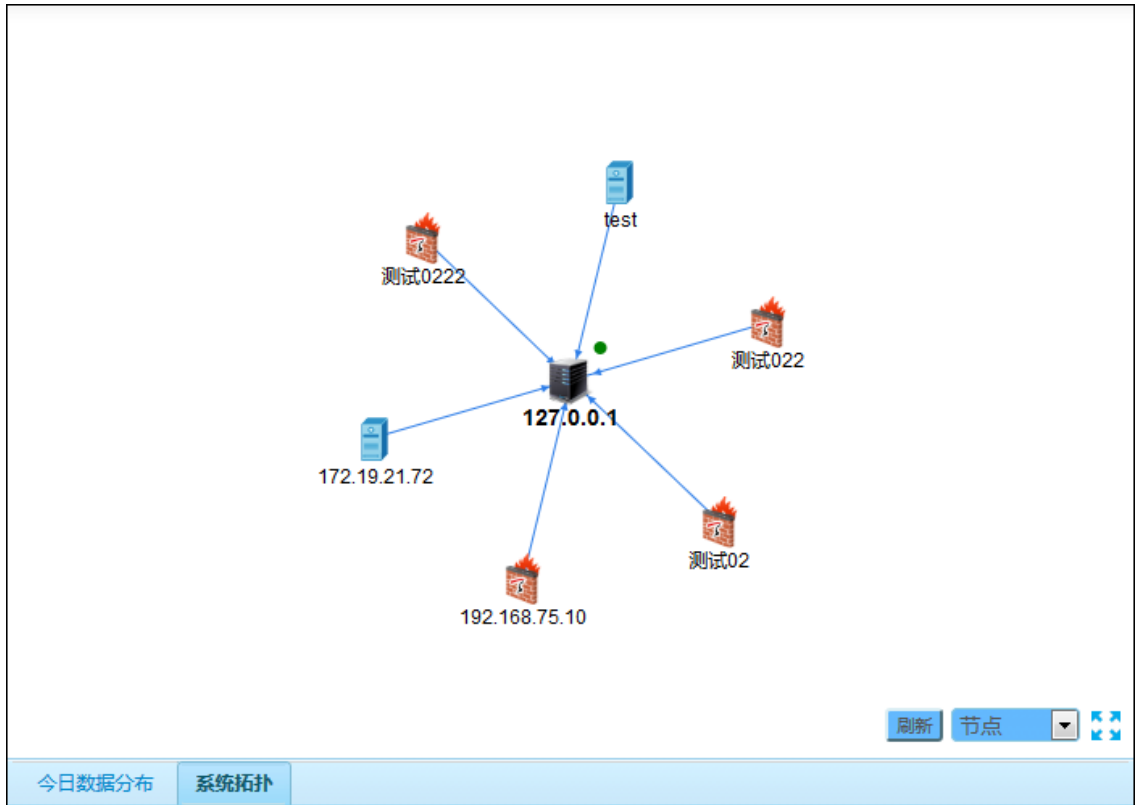


(2) 在“系统拓扑”中，右键单击监视对象，可查看该节点或者日志源的日志信息、报表和告警信息。如下图所示。



(3) 在“系统拓扑”中，用户可以按住鼠标左键不放拖动整个拓扑图或者拖动某个监视对象，同时可以点击“”图标全屏查看拓扑图。另外，用户还可以在界面右下角选择不同视角查看拓扑图，可选视角有节点、业务组和设备类型。如下图所示。


**需要说明的是**，非系统预置操作管理员（operator）没有“业务组”视角选项。



- 日志总量统计

此部分按设备类型分类统计日志数量和日志大小的信息。如下图所示。

日志总量统计		
名称	数量(条)	大小
网御神州SecGate 3600	2483.2万	9.9 GB
微软Windows系列服务器	38.7万	166.3 MB
127.0.0.1	38.7万	166.3 MB
172.19.8.14	31.5万	145.3 MB
192.168.75.10	7.2万	21.0 MB
绿盟ADS	20.9万	34.6 MB
127.0.0.1	20.9万	34.6 MB
172.16.15.58	11.3万	18.9 MB
172.16.15.59	9.6万	15.7 MB
天融信NGFW	17.3万	26.0 MB
深信服代理网关	13.2万	12.8 MB
127.0.0.1	13.2万	12.8 MB
172.16.8.168	13.2万	12.8 MB
系统日志	12.2万	27.0 MB
天融信僵木蠕	8.2万	50.3 MB
127.0.0.1	8.2万	50.3 MB
<b>总计</b>	<b>2599.3万</b>	<b>10.2 GB</b>

点击“”可以切换节点视角展示日志总量。此外还可以导出日志总量统计信息（excel 格式）。如下图所示。



日志总量统计		
名称	数量(条)	大小
127.0.0.1	2596.1万	10.2 GB
192.168.75.10	3.3万	6.4 MB
<b>总计</b>	<b>2599.3万</b>	<b>10.2 GB</b>

● 今日最新告警 Top10


该区域以列表形式显示今日最新告警详细信息，以时间倒序排列显示。如下图所示。

需要说明的是，非系统预置操作管理员（operator）没有“操作”字段。

时间	级别	告警名称	节点	设备地址	源地址	目的地址	一级分类	二级分类	操作
2017-09-15 10:30:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:29:35	中	新日志源	192.168.75.10	127.0.0.1	172.19.8.11	0.0.0.0	TSM	TopAnalyzer	
2017-09-15 10:29:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:29:18	中	连续上报告警	127.0.0.1	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer	
2017-09-15 10:28:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:27:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:26:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:25:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:24:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	
2017-09-15 10:23:28	高	主机认证失败	127.0.0.1	127.0.0.1	172.19.8.14	192.168.23.3	TSM	TopAnalyzer	

(1) 点击级别或者告警名称可以级别或者告警名称为查询条件跳转到告警查询页面。关于告警查询具体请参见 [告警查询](#) (See 5.4.3)。

(2) 点击源地址或目的地址可以源地址或者目的地址为查询条件跳转到日志查询页面。关于日志查询具体请参见 [日志查询](#) (See 5.2.3)。

(3) 点击源地址或目的地址旁边的“”，可展示出以该 IP 为源（目的）的日志查询结果的树型展示图。如下图所示。



(4) 在告警信息所在行的右侧点击“🔔”，在弹出的页面中可以关联告警，关于告警方式详细请参见 [告警方式管理](#) (See 5.7.3.4)。如下图所示。

名称	响应方式	创建者	状态
邮件告警	声音响应	operator	启用
<input checked="" type="checkbox"/> test	执行本地命令	operator	禁用
<input type="checkbox"/> rere	声音响应	operator	启用

默认 ▾

确定 取消

(5) 在告警信息所在行的右侧点击“🚫”，即可屏蔽此告警，同时系统会自动添加一条告警过滤规则，管理员可以通过选择 [告警过滤规则](#) (See 5.7.3.3)，在告警过滤规则配置列表中查看该告警过滤规则。如下图所示。

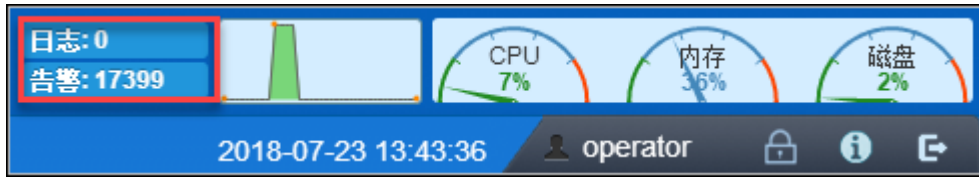
告警名称	设备地址	源地址	目的地址	告警描述	时间间隔(分钟)	速度	状态	操作
<input type="checkbox"/> 日志重复		192.168.78.31	192.168.1.65		60	0	启用	
<input type="checkbox"/> 主机认证失败		172.19.8.14	123.36.32.23		60	0	启用	
<input type="checkbox"/> 主动日志源异常		152.36.25.36	127.0.0.1		60	0	启用	
<input type="checkbox"/> 主动日志源异常		192.168.75.50	127.0.0.1		60	0	启用	
<input type="checkbox"/> 主机认证失败		172.19.8.14	192.3.16.1		60	0	启用	




🔍 只允许对本级节点产生的告警执行关联告警方式操作或者执行屏蔽此告警操作。

● 右上方快捷功能区


从首页的右上方可以查看本级今日日志总数和今日告警总数以及实时的日志流量情况，可点击“告警”查看今日告警信息列表。还可以查看系统当前的 CPU、内存和磁盘的使用率情况。如下图所示。




◇磁盘显示的是日志存储路径所在磁盘的使用率情况。

(1) 点击“”图标，可以查看当前在线的用户列表，如下图所示。

用户名	登录地址
dcc	192.168.75.51
hhh	192.168.25.103
operator	192.168.25.102

(2) 点击“”图标可以查看产品版本信息和产品许可信息，也可下载采集代理和告警代理的安装包。具体操作请参见 [关于](#) (See 5.8)。

(3) 点击“”图标可以锁定当前查看页面，具体请参见 [锁定](#) (See 5.9)。

(4) 点击“”图标，可以退出当前系统。

### 查看本级节点的详细信息

天融信日志收集与分析系统多级部署的情况下，用户不仅可以查看所有节点的信息，还可以只查看本级节点的信息，选择 **主页 > 本级**，如下图所示。



## 5.2 日志

通过配置日志源（日志源配置请参见 [日志源](#) (See 5.5)），系统能够收集到安全设备、网络设备、主机及应用服务等资产的日志信息。同时，系统还提供了多样、灵活的日志信息查询功能，可根据用户的设定，进行不同条件的日志查询，进而帮助管理员全面、深入的分析事件。灵活的查询方式帮助用户取证定位分析，为决策提供依据。

相关内容包括：

- [日志摘要](#) (See 6.1)：显示日志的概览信息。
- [实时日志](#) (See 5.2.2)：查看本级的实时日志。
- [日志查询](#) (See 5.2.3)：按日志类型和业务组进行日志查询。
- [备份管理](#) (See 5.2.4)：管理日志备份文件。
- [查询统计](#) (See 5.2.5)：自定义统计查询日志信息。

### 5.2.1 日志摘要

日志摘要模块主要显示日志概要统计信息，并以柱状图和表格的形式显示各个节点的日志大小数量统计，支持按照节点或日志源查看日志数量和大小。

**需要注意的是**，普通的操作管理员没有权限查看该页签的内容。



具体操作步骤如下：

**步骤 1** 选择 **日志 > 日志摘要**，如下图所示。



柱状图显示不同节点的日志数量和大小统计信息；表格显示不同节点的日志源的日志数量和大小统计信息。

**步骤 2** 输入年份、月份、日、节点和日志源来查询自己所需的日志信息，点击【查询】按钮即可查询，符合条件的日志会以图表的形式展现；点击【导出】按钮可将查询结果以 Word 的形式导出。

**步骤 3** 点击柱状图右上角的“”图标可以饼状图的形式显示统计查询结果；点击“”图标可将统计图保存为图片。

## 5.2.2 实时日志

实时日志功能，可以帮助管理员按照不同的日志源或设备类型进行日志监视，进而正确掌握系统的日志采集情况。可清空当前缓存中的日志，可停止刷新、手动启动刷新，操作方便灵活。



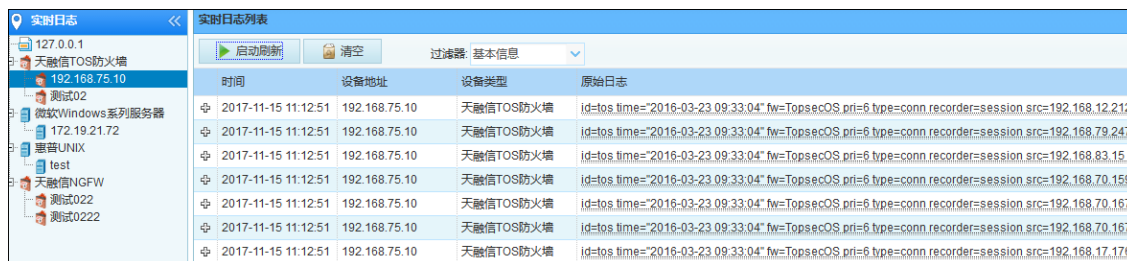
◇进入实时日志界面时，由于系统后台需要搜集日志，界面显示会有几秒钟的延迟，请等待几秒。

◇“实时日志”功能需要占用大量系统资源，因此只能进行独占操作，即在同一时间内只能由一个操作管理员对其进行查看，当前用户退出该功能 30s 后，下个用户才可进行查看。

◇实时日志只能查看本级的日志信息，不支持查看多级的实时日志信息。

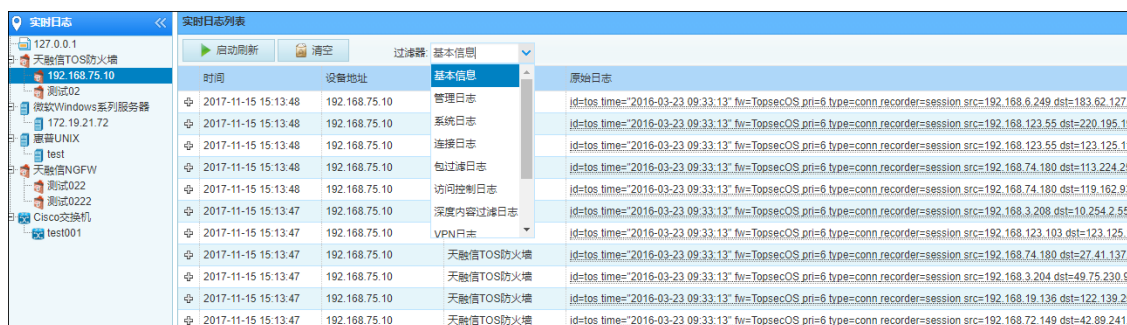
具体操作步骤如下：

**步骤 1** 选择 日志 > 实时日志，并在左侧导航树中选择要查看的日志源，几秒后右侧页面将显示实时收到的该日志源或设备类型的日志信息，如下图所示。



点击【停止刷新】按钮可以停止对日志进行实时刷新；点击“+”可以查看原始日志，鼠标悬停在指定日志所在行的原始日志操作列可显示日志的详细信息。

**步骤 2** 在“实时日志”过滤器下拉列表中显示了某种日志源的不同列集，选择不同的过滤器，可以对系统的实时日志进行过滤显示，如下图所示。

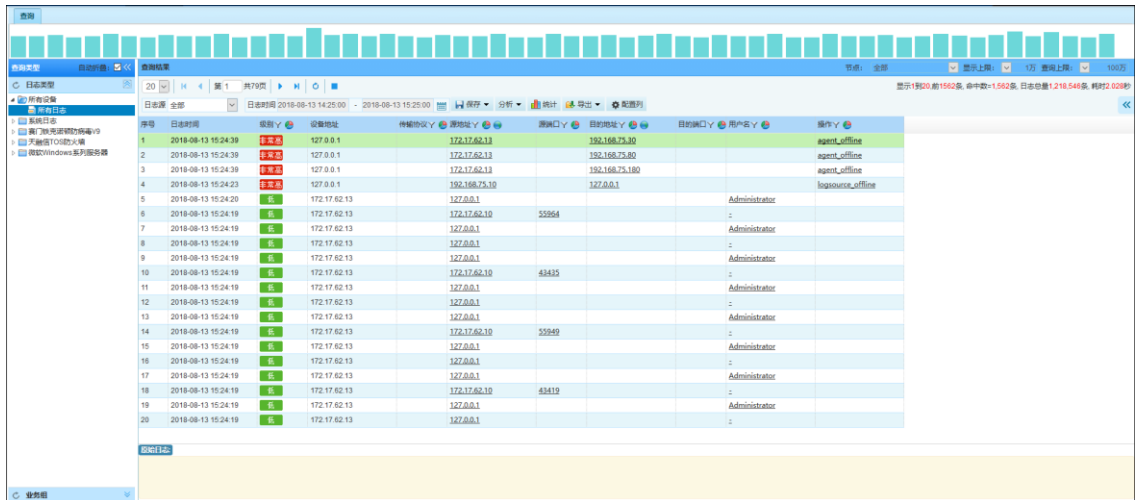


**步骤 3** 点击日志列表上方的【清空】按钮可以清空当前页面中的日志列表，清空缓存中的数据，开始重新监视。


## 5.2.3 日志查询

系统的日志查询功能支持按照“日志类型”和“业务组”两个视角进行日志查询（非系统预置的操作管理员不支持“业务组”的视角查看日志信息），并进一步设置详细查询条件灵活查询系统收集到的所有设备的日志，查询的结果会以表格的形式显示在页面中，同时页面上方会以柱状图的形式直观展示，主要查询条件包括：日志源、时间、节点和显示、查询上限，其中“节点”查询参数只有在有下级节点的设备界面中出现，关于日志源的配置请参见 [日志源](#) (See 5.5)。同时系统支持对查询结果进行可视化展示，展示给用户的图表种类丰富多样，主要有：树图、散点图、关系图、折线图、时序表和柱状图。

**步骤 1** 选择 **日志 > 日志查询**，进入日志查询页面，在左侧导航树选择要查询的日志类型，默认显示最近一小时时间间隔内的日志信息，如下图所示。



同时，系统支持按业务组进行日志查询，关于业务组的相关操作具体请参见 [业务组](#) (See 5.5.2)（只有系统预置的操作管理员有权限查看“业务组”页签）；点击页面

右侧的“”按钮可显示最近 14 条查询条件，如需再次查询，可点击指定查询条件进行快速查询。

IP 地址为公网地址的系统会自动识别地址，并在 IP 地址前标有该 IP 地址所在国家的国旗；内网地址则没有标识。

页面上方以柱状图的形式显示更小时间间隔内的设备日志信息，鼠标悬停任意点击；页面中部以列表的形式显示符合查询条件的日志信息；页面底部显示当前日志对应的原始日志。

## 步骤 2 设置基础查询条件。

1) 点击相应下拉框选择日志源、查询时间范围、节点、显示上限和查询上限（节点、显示上限和查询上限三个字在页面右上角的位置），设置完成后，查询条件立即生效，查询结果实时刷新。管理员可通过点击【配置列】按钮，来选择显示在查询结果列表中的字段。



柱状图的横坐标是管理员将指定的查询时间间隔细分出的更小时间间隔，具体划分函数请咨询天融信技术支持人员。

柱状统计图和表格显示的结果和“显示上限”有关，即显示的是界面中显示出来的日志的信息，而非查询出来的日志信息。

由于对查询结果显示的日志进行统计时会消耗系统资源，当要统计的日志数量较大时，对系统资源消耗较大，降低系统性能。

因此，请根据系统的性能配置“显示上限”和“查询上限”。

2) 点击【保存】按钮，弹出“保存条件”窗口，如下图所示。



设置名称和需要保存的查询条件（需查询的日志的时间范围），设置完成后，点击【保存】按钮，即可保存查询条件。成功保存后，鼠标悬停在【保存】按钮上时可显示，如需再次查询，直接点击即可。保存成功后的效果图如下图所示。

✓	hxj1	
	hxj	

保存的查询条件前有对勾的是最近一次执行过的查询条件。

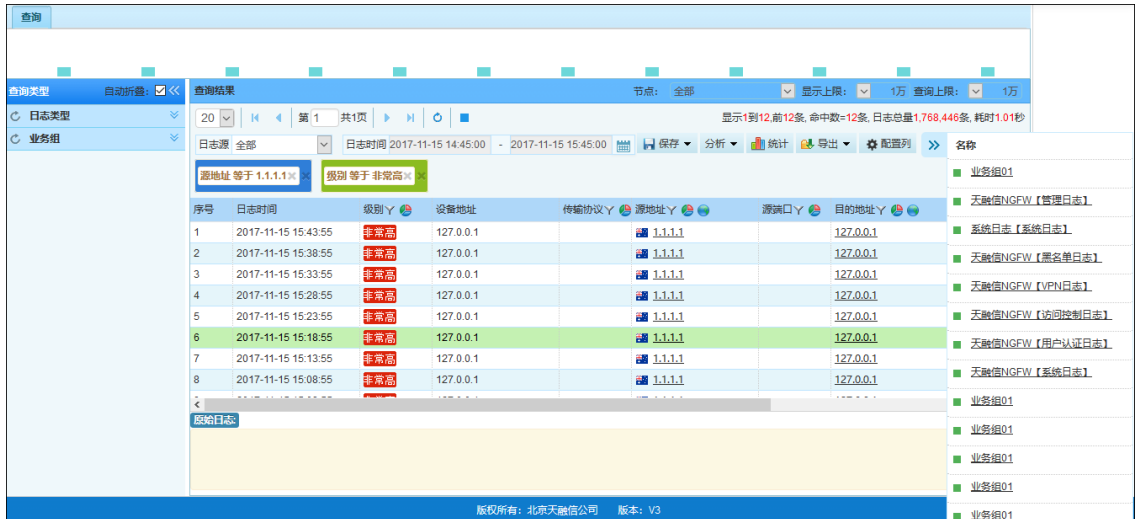
5) 点击【统计】按钮，可跳转至创建主题页面，可对当前的查询结果进行自定义统计，关于统计主题的创作，请参见 [统计主题](#) (See 5.2.5.1)；点击【导出】按钮可按需导出相应的原始或格式化日志（支持 Excel 和 CSV 格式）；点击【配置列】按钮可选择显示在界面上的日志字段。

### 步骤 3 设置高级查询条件。

1) 点击“”图标，打开对话框选择查询条件（“等于”、“不等于”、“大于”、“小于”、“正则表达式”）和查询属性（属性值或关键字），多个属性值或关键字间使用逗号分隔。

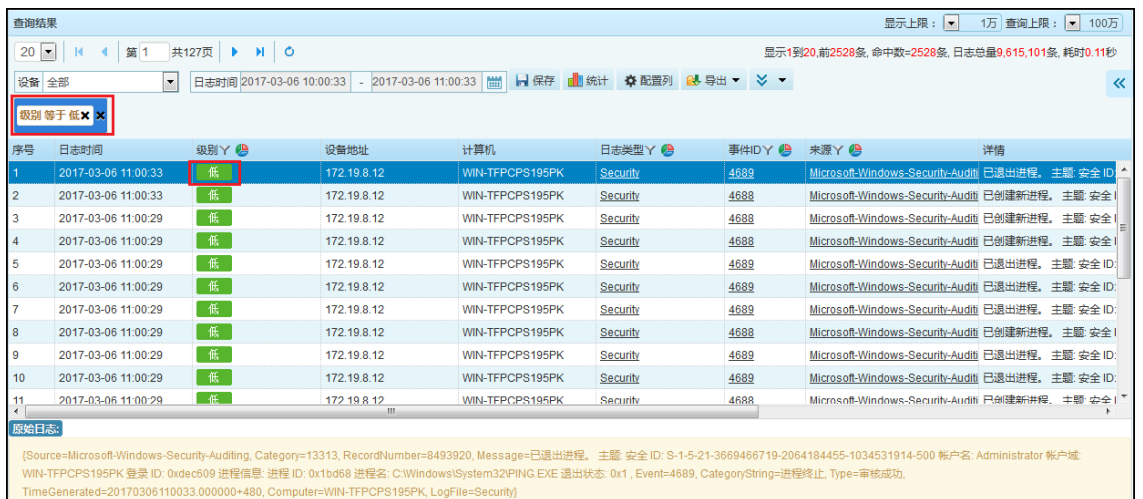
2) 不同的字段名可选择的查询条件不同，设置完成后，点击【确定】按钮可在结果列表上方以不同颜色显示已设置的查询条件，查询结果同时显示，可再次点击有下划线的字段（包括已经点击的字段）继续快捷查询，本次查询的字段与上一次查询的字段之间是“与”的关系。如下图所示。





#### 步骤 4 日志快捷查询。

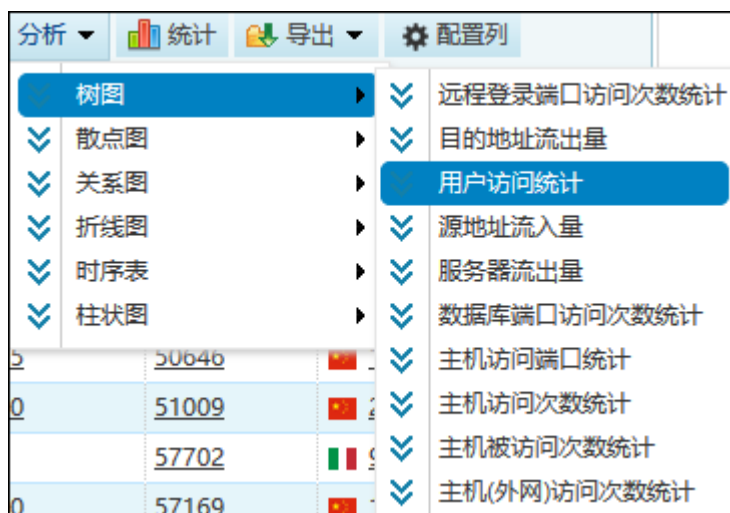
点击查询列表中有下划线的字段值，可将相应字段值作为查询条件，进行快捷查询。  
例如：点击表中级别为“低”的字段，查询列表即显示所有级别为“低”的日志，如下图所示。



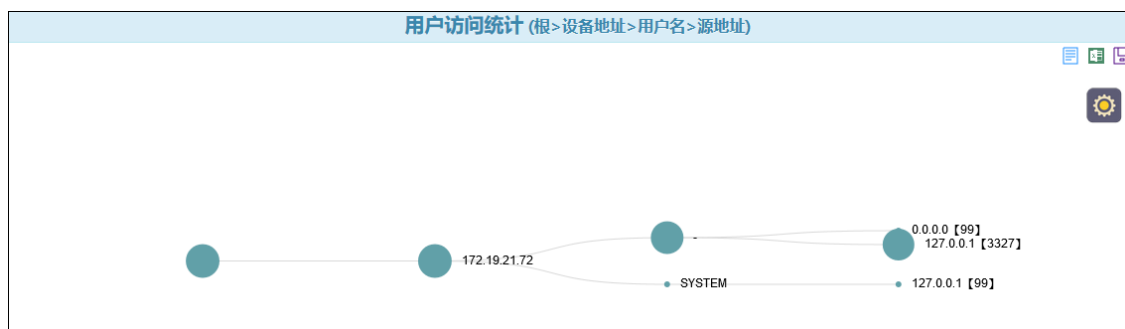
#### 步骤 5 查询结果可视化展示。

1) 对查询结果进行多维度展示。

a) 点击日志查询页面的【分析】按钮可基于当前的查询结果进行可视化图表展示，图标类型主要有以下几种。



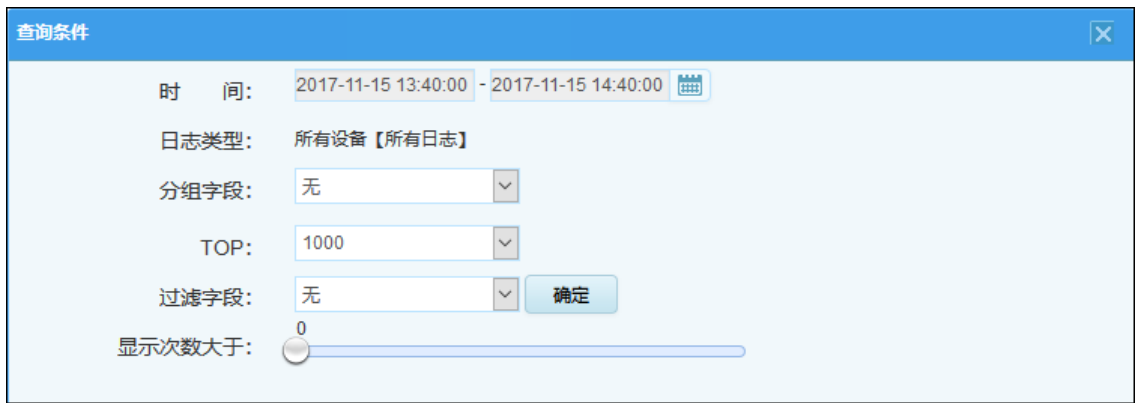
b) 关于图表的操作类似，在此以树图为例进行介绍，如上图所示，选择一个字段（此处以用户访问统计为例），完成之后进入用户访问统计页面，如下图所示。



鼠标悬停在树图圆点，会显示详细信息，包括设备地址、用户名、源地址和次数，点击树图中任意圆点会下钻到日志查询界面，以该圆点 IP 地址为查询条件显示日志统计结果。

点击右上角的“📄”图标，可将树图切换为列表视图；点击右上角的“📄📄”图标，可将树图导出为 Excel 格式；点击“🖨️”图标，可将图表保存为图片。

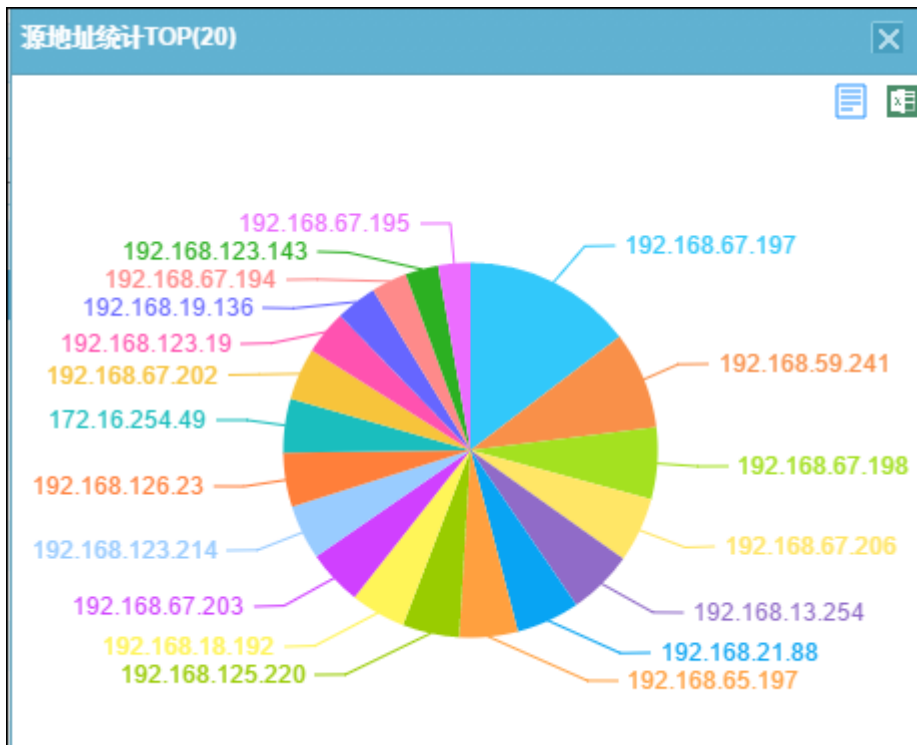
c) 整个树图包括跟、设备地址、设备名和源地址，鼠标悬停在图中的圆点处可显示详细信息；点击“⚙️”图标（也可双击空白处），弹出“查询条件”窗口，如下图所示。



可在该窗口设置树图显示的日志的信息，参数如上图所示。

2) 查看 TOP 统计排行。

a) 点击查询结果列表有“🌐”标识的字段，弹出 TOP 排行统计结果。系统默认以饼状图形式展示统计结果，如下图所示。





b) 点击右上角的“📄”图标，统计结果切换为列表视图；点击右上角的“📄”图标，可将统计结果导出为 Excel 格式。

3) 查看源/目的地址在全国或全球的数量分布。

a) 点击源地址/目的地址右侧的“🌐”，可弹出相应的源/目的地址数量分布面板，现以源地址数量分布面板为例，如下图所示。



上图显示查询结果中源 IP 地址在全国或全球的数量分布，可点击“全国数量分布”或“全球数量分布”进行查看，鼠标悬停图中会显示详细信息；点击右上角的“”图标，统计信息切换为列表视图；点击右上角的“”图标，可将统计信息导出为 Excel 格式。

## 5.2.4 备份管理

备份管理模块支持对 TA-L 收集到的日志进行备份，以便需要时进行日志备份的导入导出操作；同时提供了第三方日志导入和管理主机本地导入的入口。

相关内容包括：

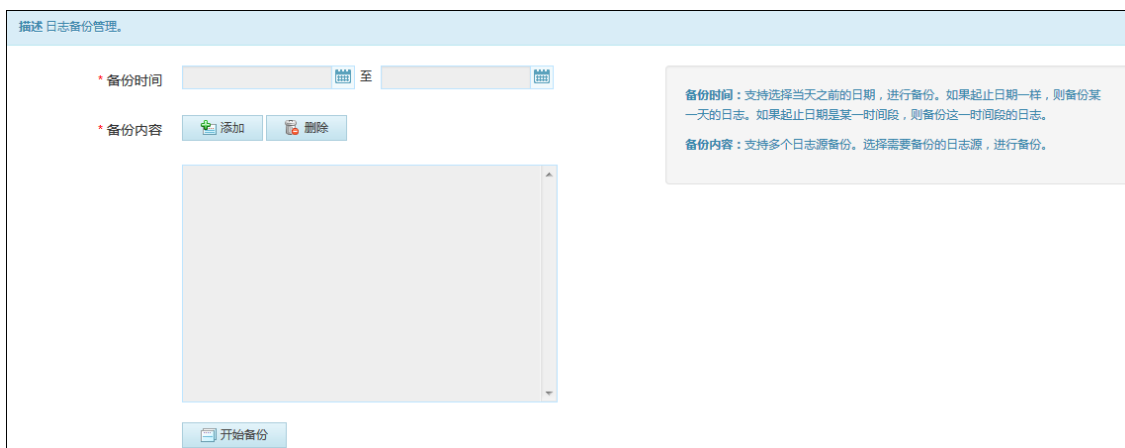
- [日志备份](#) (See 5.2.4.1)：备份日志，支持对多个日志源进行备份，备份的文件会显示在“备份导入”页签的 **备份文件** 列表处。
- [备份导入](#) (See 5.2.4.2)：备份日志导入，主要包括：系统备份文件导入、服务器本地文件导入和客户端本地文件导入三种方式。

### 5.2.4.1 日志备份

管理员可以对系统中的日志进行手动备份，系统可以将日志备份到本地或 FTP 服务器上。

进行日志备份的具体操作为：

**步骤 1** 选择 **日志 > 备份管理**，进入手动备份设置界面，如下图所示。



设置手动备份参数时，各项参数的具体说明如下表所示。

参数	说明
备份时间	选择备份的开始时间和结束时间。
备份内容	点击【添加】按钮，在弹出的对话框中选择要备份日志的日志源，有关日志源的设置请参见 <a href="#">日志源</a> (See 5.5)。

参数设置完成后，点击【开始备份】按钮即可提交备份任务，提交的备份任务步骤可激活“备份导入”页签进行查看，有关备份导入的具体操作请参见 [备份导入](#)(See 5.2.4.2)。

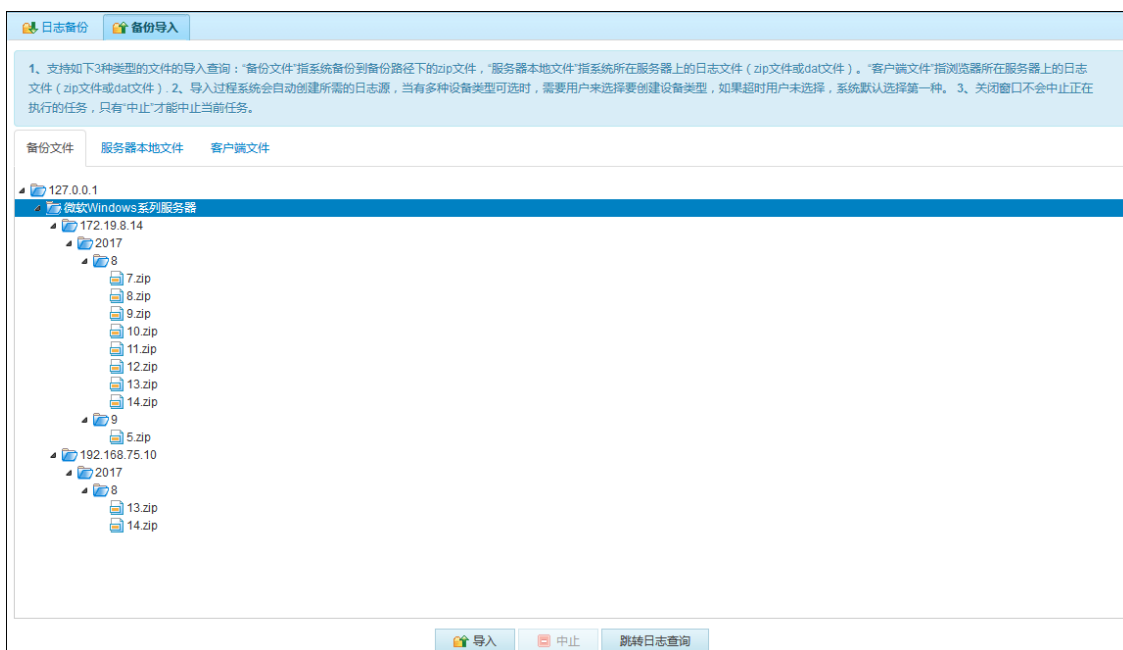


◇ 如果选择的起止时间一样，则备份某一天的日志。

## 5.2.4.2 备份导入

在查询历史日志之前，首先要导入历史日志。系统支持三种导入方式：备份文件导入、服务器本地文件导入和客户端文件导入，方便管理员进行离线分析和远程管理。其中，备份文件是指将系统日志备份到指定的备份路径下，通常是.zip文件；服务器本地文件是指系统所在服务器上的日志文件，格式为.zip或.dat文件；客户端文件是指浏览器所在主机上的日志文件，格式为.zip或.dat文件。三种备份导入方式操作步骤大体相同，现以备份文件导入为例：

**步骤 1** 选择 **日志 > 备份管理**，激活“备份导入”页签，进入备份导入页面，如下图所示。



页面中显示的是系统的备份文件，关于系统文件的备份请参见 [日志备份](#) (See 5.2.4.1) 和 [备份策略](#) (See 5.7.1.2)。

选择需导入的备份文件，点击【导入】按钮即可导入备份文件，如需中止，点击【中止】按钮中止导入操作。如需查询所需日志，可点击【跳转日志查询】按钮快速跳转到日志查询界面。

## 步骤 2



❖ 关闭备份文件导入窗口，导入操作不会中止，需点击【中止】按钮。

## 5.2.5 查询统计

统计主题，可以满足用户对历史日志统计分析的需求。在这里可以弥补报表中内置统计主题的不足，当报表中的主题无法满足报表统计需要时，可以在这里自定义统计主题，对指定时间指定查询条件的日志进行统计。系统支持对查询统计事件进行日志审计，记录审计日志，可登录审计管理员（auditor）进行查看。有关统计任务的配置具体请参见 [统计任务](#) (See 5.2.5.2)。

相关内容包括：

- [统计主题](#) (See 5.2.5.1)：自定义统计主题，执行统计任务时引用创建的统计主题。
- [统计任务](#) (See 5.2.5.2)：自定义统计任务，查询所需日志信息。

## 5.2.5.1 统计主题

本节介绍如何对已创建的统计主题进行管理，包括新建主题、主题执行、编辑、删除、预览和导出 Excel 操作。具体操作如下：

**步骤 1** 选择 **日志 > 查询统计**，激活“统计主题”页签，进入统计主题列表，如下图所示。

名称	时间间隔	开始时间	结束时间	状态	进度(%)	结果类型	TOP	操作
天融信TOS防火墙								
topic1	最近一周	2017-11-14 15:22:01	2017-11-14 15:22:03	执行成功	100	柱图	5	
topic2	最近一周			未执行		表格	5	
微软Windows系列服务器								
11	最近一周	2017-11-14 15:36:08	2017-11-14 15:36:10	执行成功	100	柱图	5	

**步骤 2** 点击【新建】按钮，弹出“创建主题”的对话框，如下图所示。

新建
删除
刷新

名称	时间间隔	开始时间	结束时间	状态	进度(%)	结果类型	TOP	操作
天融信TOS防火墙								
topic1	最近一周	2017-11-14 15:22:01	2017-11-14 15:22:03	执行成功	100	柱图	5	
topic2	最近一周			未执行		表格	5	
微软Windows系列服务器								
11	最近一周	2017-11-14 15:36:08	2017-11-14 15:36:10	执行成功	100	柱图	5	

主题名称:

时间间隔: 自定义 ▼

选择方式: 节点 ▼

节点: 请选择 ▼

日志类型: 请选择 ▼

日志源: 请选择 ▼

日志列表: 请选择 ▼

过滤条件: 级别 ▼ 等于 ▼ 非常低 ▼ +

**分组字段**

字段名称	分组方式
<input type="checkbox"/> 日志时间	无 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 级别	
<input type="checkbox"/> 设备地址	无 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 事件名	
<input type="checkbox"/> 传输协议	
<input type="checkbox"/> 源地址	无 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 源网段	
<input type="checkbox"/> 源国家	
<input type="checkbox"/> 源省份	
<input type="checkbox"/> 源城市	

**统计字段**

字段名称	统计方式
<input type="checkbox"/> 日志时间	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 级别	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 设备地址	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 事件名	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 传输协议	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 源地址	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 源网段	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 源国家	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 源省份	次数 <span style="font-size: small;">▼</span>
<input type="checkbox"/> 源城市	次数 <span style="font-size: small;">▼</span>

**排序**

字段名称	次序	操作

**结果类型**

结果: 柱状图 ▼

TOP: 5 ▼


横轴: ▼

保存 取消

在设置统计条件时，各项参数的具体说明如下表所示。

参数	说明
主题名称	设置统计主题的名称。
时间间隔	选择此次统计的日志的时间范围。
节点	选择需要进行日志统计的节点。

70

参数	说明
日志类型	选择需统计的日志类型。
日志源	选择需统计的日志源。
日志列集	选择日志列集，不同的日志类型，日志列集的字段会有所不同，具体以产品界面为准。
过滤条件	<p>设置日志的过滤条件，支持依据级别、模块、操作、用户名和结果进行过滤日志，一条过滤条件设置完成后，点击  图标可增加一条过滤条件，如需增加多条，重复此操作即可，多个过滤条件之间的关系为：与。</p>
分组字段	<p>必选项，勾选一个或多个分组字段，勾选的分组字段会显示在“排序”列表中。</p> <p>说明： 选择超过三个分组字段（包括三个）时，结果类型只能选择表格； 分组方式：为日志查询时进行分组的依据，其中时间的分组方式包括年、月、日、小时和分钟，若选择的分组方式为年，则系统会将月、日、小时和分钟置为0进行日志分组查询，依次类推。</p>
统计字段	必选项，勾选一个或多个统计字段，勾选的统



参数	说明
	计字段会显示在“排序”列表中。
排序	勾选的分组字段和统计字段会显示在该列表中，点击指定的排序字段操作列的“↑”或“↓”可上移或下移排序字段的位置，此处的顺序影响结果类型中TOP统计结果的显示。
结果类型	选择统计日志源的Top条数，包括5、10、30、50、100、1000、10000，并选择横轴以及显示形式，显示形式包括：柱状图、曲线图、饼图、表格。

添加成功后，分别点击某个主题名称所在行的“🔄”、

“▶”、“✎”、“🗑️”、“📄”、“📄”可完成

**步骤 3** 刷新主题、执行主题、编辑主题、删除主题、预览统计结果、以表格形式导出统计结果的操作。

选中多个统计主题，点击页面上方的【删除】按钮可批量删除统计主题；点击【刷新】按钮可立即刷新主

**步骤 4** 题列表。



不同的操作管理员创建的统计主题对彼此都是不可见的，系统预置的操作管理员也是没有权限的。

编辑修改统计主题名称后，之前的统计结果将无法预览，只有在主题再执行一次后方可进行预览。

## 5.2.5.2 统计任务

统计任务与自定义报表功能类似，其灵活度和可操作性更高。支持将多个统计主题组合到一起，建立统计任务，生成综合报表可以在线预览，也可以直接下载到本地或发送到指定邮箱。统计任务可设置为周期性执行，也可指定时间执行。具体操作步骤如下：

选择 **日志 > 查询统计**，点击“统计任务”页签后进入页面。该页面列出在查询统计页面中设置完成的统计任务列表，如下图所示。

**步骤 1**

名称	执行状态	执行周期	开始时间	结束时间	创建人	状态	操作
task2	执行完成	分钟间隔	2017-09-18 16:40:00	2017-09-18 16:55:30	operator	启用	[操作图标]
task1	执行完成	分钟间隔	2017-09-21 13:30:00	2017-09-21 13:30:11	operator	启用	[操作图标]
task0	执行完成	分钟间隔	2017-09-21 13:30:00	2017-09-21 13:30:14	operator	启用	[操作图标]
h1	等待执行	分钟间隔			operator	禁用	[操作图标]

步骤 2 点击【创建任务】按钮，进入创建统计任务的界面，如下图所示。

名称: task01

邮箱地址: zhangsan@163.com

执行周期: 分钟间隔 (10 分)

主题名称	节点	业务组	日志源	时间间隔	结果类型	TOP	操作
11	127.0.0.1		微软Windows系列服务器	最近一周	柱图	5	[操作图标]

1、多个邮箱使用分号隔开

2、点击时间间隔表格自定义时间间隔

3、如果时间间隔选择自定义，需要点击选择时间范围

4、单击会应用此主题的时间间隔到所有主题

5、选择主题会清空当前主题，使用新选择的主题


在创建统计任务时，各项参数的具体说明如下表所示。

参数	说明
名称	设置统计任务的名称。
邮箱地址	添加统计结果收信人的地址，格式如： <a href="mailto:abc@topsec.com.cn">abc@topsec.com.cn</a> 格式，多个邮箱地址用英文的分号隔开。
执行周期	设置执行任务的时间，包括：分钟、小时、日、周、月，其中间隔分钟数不能小于 10。
选择主题	点击【选择主题】按钮，在打开的主题页面中选择需要统计的主题内容，选定后自动填入下方列表中。 说明： 之前选择的统计主题会被清空，使用新选择的统计主题。
增加主题	点击【增加主题】按钮，在打开的主题页面中选择需要统计的主题内容，选定后自动填入下方列表中。

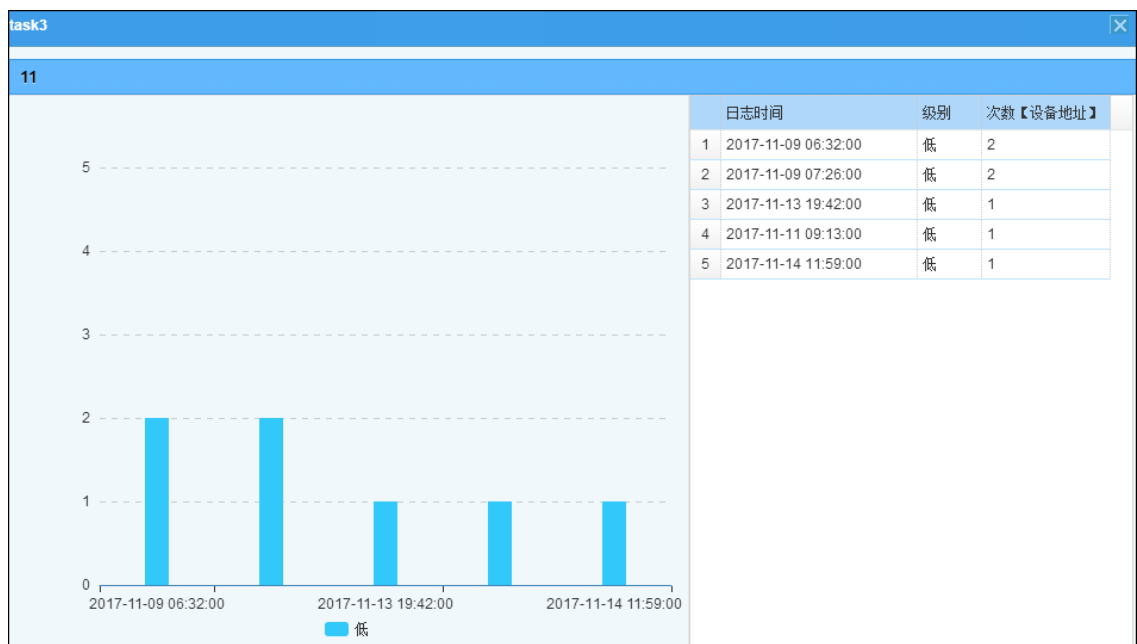
参数	说明
	<b>需要说明的是：</b> 点击主题列表处的“时间间隔”字段，可自定义设置日志统计的时间范围。


参数设置完成后，点击【保存】按钮




**步骤 3** 完成统计任务的创建。


统计任务执行成功后，点击指定统计任务所在行的“”可预览统计结果，如下图所示。

**步骤 4**



如需对已创建完成的统计任务进行编辑，可点击相应统计任务右侧的“”按钮进行

编辑；点击“”或“”按钮可在启用和禁用统计任务间进行切换；点击“”按

**步骤 5** 钮可进行批量下载；点击“”按钮可将统计任务执行结果以 Word 格式导出。

历史文件			
批量下载			
<input type="checkbox"/>	文件名称	创建日期	操作
<input type="checkbox"/>	20170918165535.doc	2017-09-18 16:55:35	
<input type="checkbox"/>	20170918164534.doc	2017-09-18 16:45:34	
<input type="checkbox"/>	20170918163557.doc	2017-09-18 16:35:57	
<input type="checkbox"/>	20170918162540.doc	2017-09-18 16:25:40	
<input type="checkbox"/>	20170918161624.doc	2017-09-18 16:16:24	
<input type="checkbox"/>	20170918160541.doc	2017-09-18 16:05:41	
<input type="checkbox"/>	20170918155605.doc	2017-09-18 15:56:05	
<input type="checkbox"/>	20170918154537.doc	2017-09-18 15:45:37	
<input type="checkbox"/>	20170918153611.doc	2017-09-18 15:36:11	
<input type="checkbox"/>	20170918152549.doc	2017-09-18 15:25:49	



不同的操作管理员创建的统计任务对彼此都是不可见的，系统  
 ✧ 预置的操作管理员也没有权限查看。  
 编辑修改统计主题名称后，之前的统计结果将无法预览，只有  
 ✧ 在主题再执行一次后可预览。

## 5.3 报表

天融信日志收集与分析系统支持报表功能，可以自动对自身生成的日志及收集的日志进行详尽的分析及统计，并将分析与统计结果以丰富的报表进行多维度展示。



✧TA-L 作为下级节点时，管理员可查看本级节点的各类报表；  
 TA-L 作为管理节点时，上级管理员不仅可查看本级节点的各类  
 报表，还可查看各下级节点的各类报表。

相关内容包括：

- [基本报表](#) (See 5.3.1)：介绍如何查看、查询和导出系统自动生成的报表。
- [计划报表](#) (See 5.3.2)：介绍如何定制计划报表，使系统周期性自动生成管理员所需的报表。

---

## 5.3.1 基本报表

天融信日志收集与分析系统内置了一系列基础信息报表模板，包括系统报表模板、告警报表模板、日志报表模板和审计报表模板。系统自身产生了日志或收集到日志源的日志信息后，会根据基础信息报表模板自动生成相应的报表，并展示于其 UI 界面中。管理员可以在系统 UI 界面的 **报表 > 基本报表** 菜单中查看和查询各种类型的报表，并可将报表以 Word、PDF、Excel 和 HTML 格式导出到本地。



◇不同类型的管理员，可查看的基本报表类型不同。1) 系统预置的操作管理员“operator”可查看的报表类型包括：系统报表、告警报表和日志报表，而非预置的操作管理员可查看的报表类型只有日志报表；2) [审计管理员](#) (See 6.) 可查看的报表类型包括：审计日志报表；3) 账户管理员无报表的查看权限。  
◇对于不同的日志源设备类型，系统内置了不同的设备日志报表模板。操作管理员只有具有相应日志源设备的管理权限，才可查看该设备的日志报表。

相关内容包括：

- [系统报表](#) (See 5.3.1.1)
- [告警报表](#) (See 5.3.1.2)
- [日志报表](#) (See 5.3.1.3)

### 5.3.1.1 系统报表

天融信日志收集与分析系统通过对其自身运行期间生成的系统日志进行分析、统计，形成系统报表，报表类型包括：系统日志排行、危险级别排行和危险级别趋势报表。

- **系统日志排行**：对各种类型系统日志的条数进行统计，展示系统日志数量排名前 N 位的节点/日志类型（N 由管理员手工设置，取值可为 5 或者 10）。
- **危险级别排行**：将系统日志根据危险级别进行分类，并进行日志条数统计，展示系统日志数量排名前 N 位的节点/危险级别。
- **危险级别趋势**：根据系统日志的危险级别进行分类，并进行日志条数统计，展示相应危险级别的系统日志条数随时间的变化情况。

管理系统报表的具体操作步骤如下：

选择 **报表 > 基本报表 > 基础信息报表 > 系统报表 > 系统日志统计**，界面默认展示全部节点最近 1 小时整点时间段内的报表统计信息。在查看单个节点的报表信息时，**步骤 1** 表中会显示平均值、最高数据值和最低数据值，如下图所示。

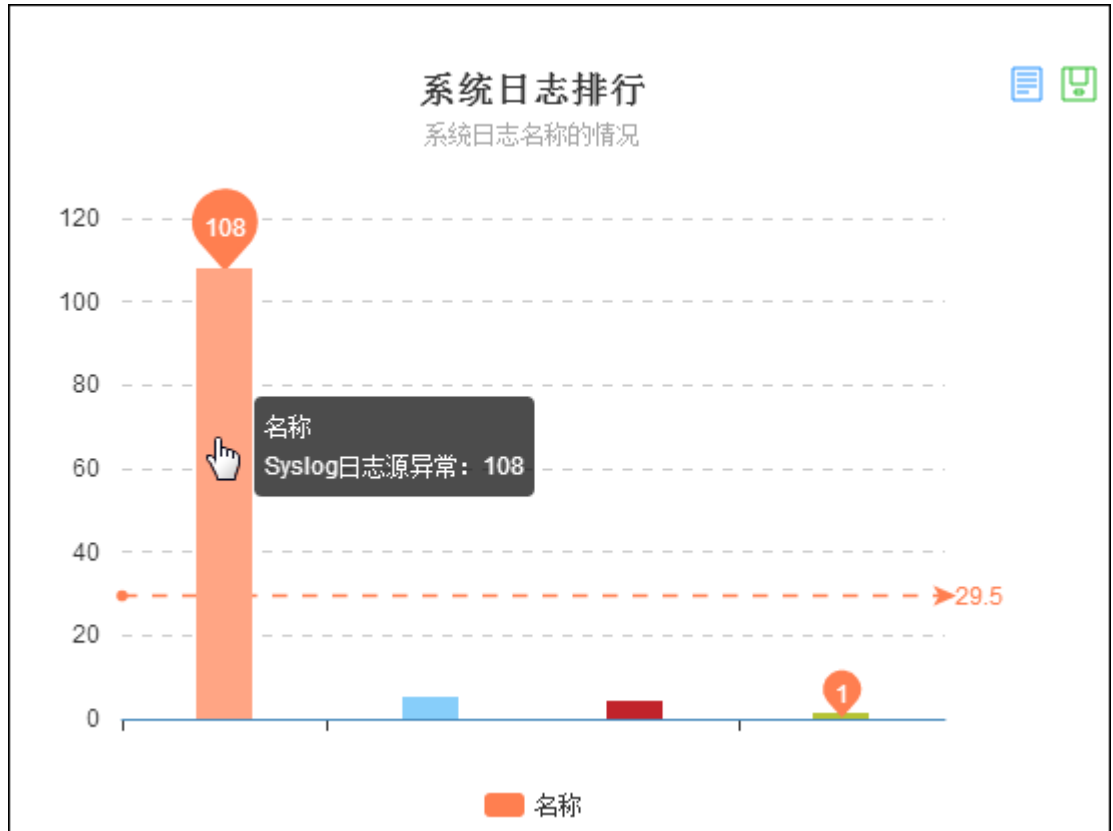


## 步骤 2 查看系统报表

系统报表包括柱状图和曲线图报表，柱状图和曲线图报表均支持以数据视图形式展示，柱状图报表包括：系统日志排行、危险级别排行；曲线图报表包括：危险级别趋势报表。柱状图和曲线图报表的查看方式稍有差异，下面分别进行介绍。

### 1) 查看柱状图报表

(a) 柱状图中的虚线表示 TOPN 系统日志数量的均值，柱状图形上通过气泡标识了 TOPN 系统日志数量的最大值和最小值。将鼠标移动到柱状图上，界面可展示相应类型系统日志的数量，如下图所示。

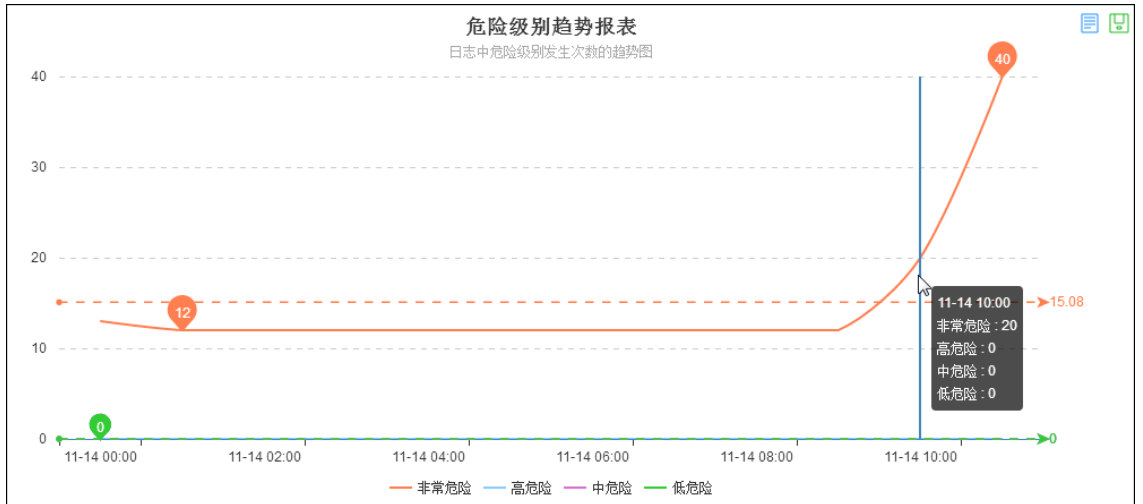


(b) 点击柱状图上相应柱状图形，可下钻到系统日志查询界面，界面默认展示与该柱状图形表示的系统日志的详细信息，关于系统日志的查看请参见 [日志查询](#) (See 5.2.3)。


## 2) 查看曲线图报表

(a) 系统日志曲线图以不同颜色的线条标识曲线类型，界面上有明确的说明，如 “**非常危险** **高危险** **中危险** **低危险**”，其中，实线表示实际的数值，虚线表示平均值。

(b) 将鼠标移动到曲线图上，界面可展示相应时间点各种类型系统日志的数量，如下图所示。



### 3) 以数据视图形式展示报表

(a) 点击相应报表类型右上角的数据视图图标“”，报表以列表的形式展示，如下图所示。

系统日志排行	
系统日志名称的情况	
名称	计数
Syslog日志源异常	180
报表	5
日志合并	4
超过存储期限	1

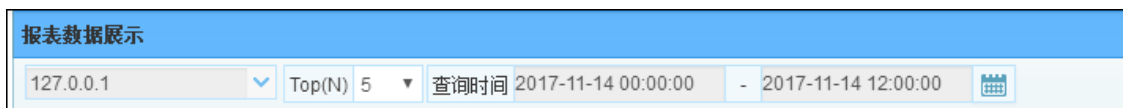
[关闭](#)

(b) 点击颜色为橙色的数据，可下钻到系统日志查询界面，界面默认展示该数据相关的所有日志信息。关于系统日志的查看请参见 [日志查询](#) (See 5.2.3)。

### 步骤 3 查询系统报表

1) 设置查询报表条件，如下图所示。






在设置查询条件时，各项参数的具体说明如下表所示。

参数	说明
节点	TA-L 作为管理节点时，可选项：全部、127.0.0.1 和节点名称，全部表示本级及下级所有节点；127.0.0.1 表示本级；节点名称表示指定的节点，关于节点的介绍请参见 <a href="#">节点管理</a> (See 5.7.3.7)。TA-L 作为下级节点时，可选项：全部，全部即表示本级节点。 说明： TA-L 的节点类型在安装 TA-L 服务器时配置，TA-L 服务器的安装过程请参见 <a href="#">安装 TA-L 服务器</a> (See 3.2.1)。
Top (N)	表示只对选定的节点中数据大小排名前 N 的系统日志进行分析统计，可选项：5、10。
时间	点击时间控件框，即可进行设置。可选项：最近一小时、今天、昨天、最近一周、最近一月、自定义，选择自定义时，可设置 1 年时间段内的任意起止时间段。

2) 设置查询条件后，系统自动进行加载和分析，形成符合查询条件的报表。

#### 步骤 4 导出报表。

1) 点击界面右上角的相应图标 “”，可将界面展示的所有报表以 Word、PDF、Excel 或 HTML 文档格式导出到本地。

2) 点击相应报表类型右上角的保存为图片图标 “”，可以将界面展示的相应报表以图片的格式 (.png) 保存到本地。

## 5.3.1.2 告警报表

天融信日志收集与分析系统通过对告警信息进行分析、统计，形成告警报表，告警报表类型包括：告警趋势报表和告警系列报表。

相关内容包括：

- [告警报表](#) (See 5.3.1.2.1)
- [告警趋势](#) (See 5.3.1.2.2)

---

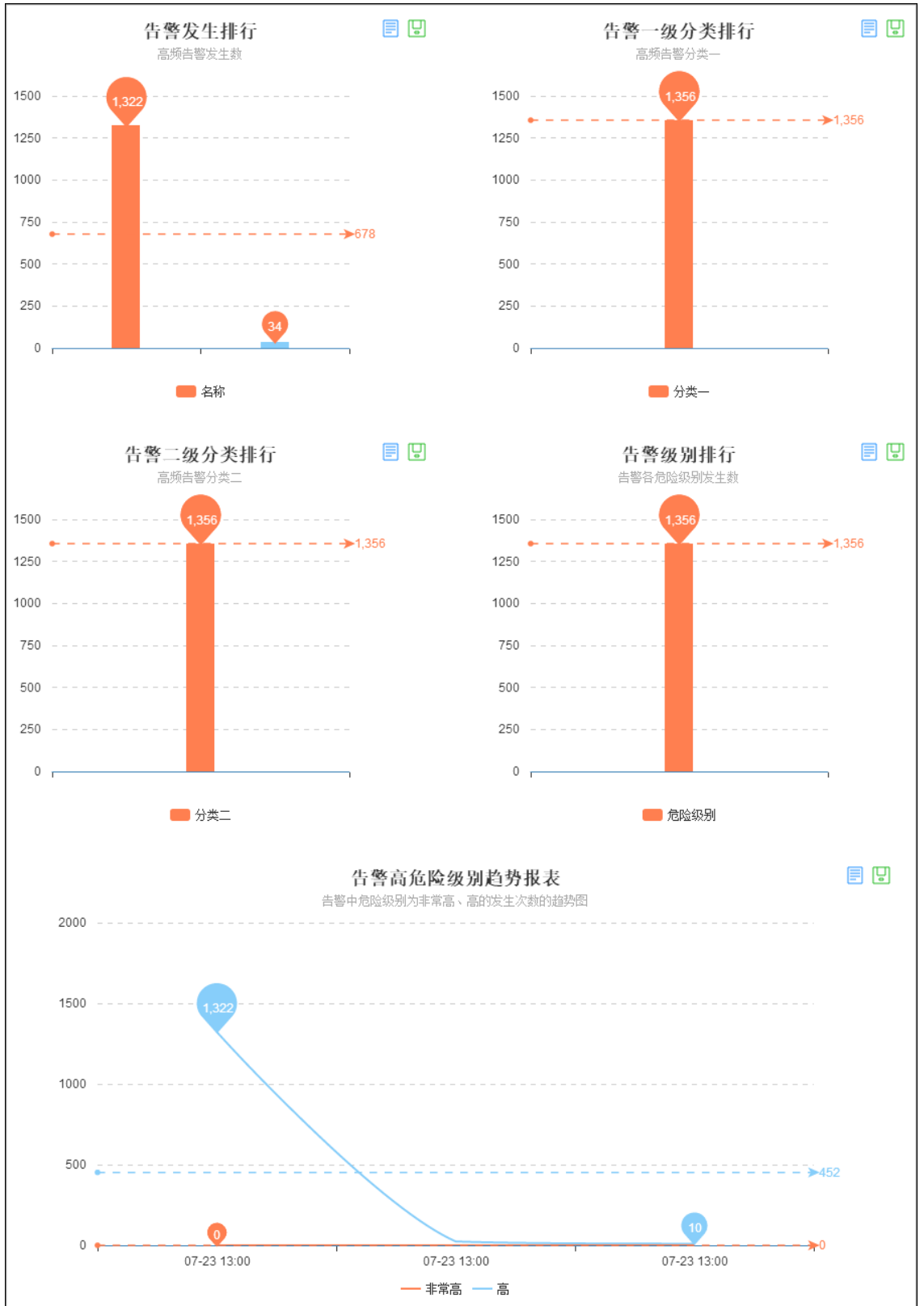
### 5.3.1.2.1 告警报表

告警报表包括：告警发生排行、告警一级分类排行、告警二级分类排行、告警级别排行和告警高危险级别趋势报表。

管理告警报表的具体操作步骤如下：

选择 **报表 > 基本报表 > 基础信息报表 > 告警报表 > 告警报表**，界面默认展示全部节点最近 1 小时整点时间段内的报表统计信息。在查看单个节点的报表信息（或不含下级节点的 TA-L 报表信息）时，报表中会显示平均值、最高数据值和最低数据值，如下图

**步骤 1** 所示。

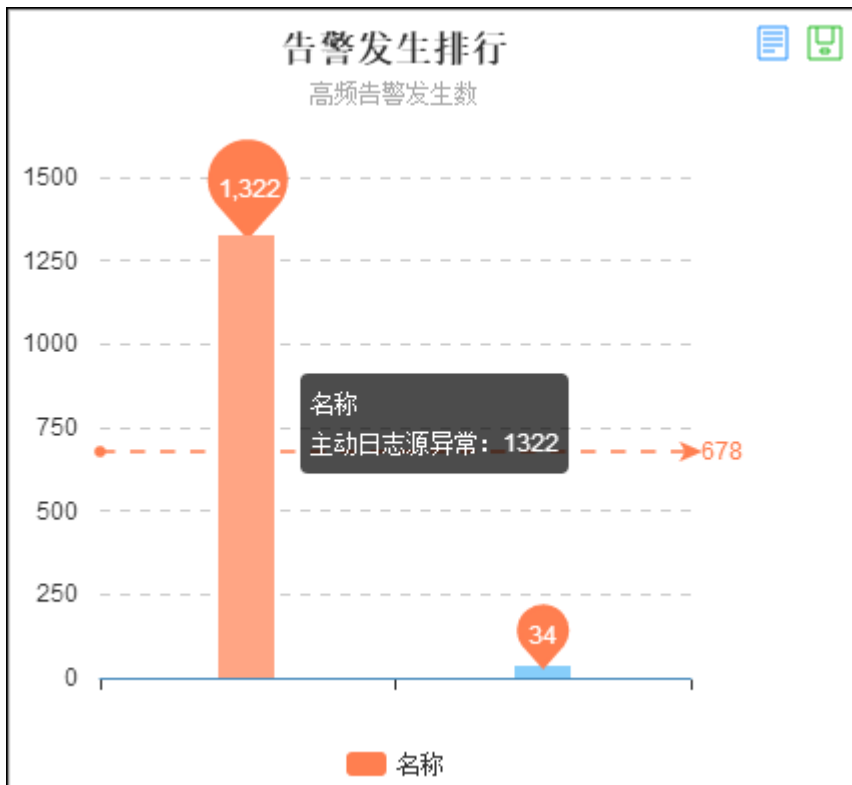


## 步骤 2 查看告警报表

告警报表包括柱状图和曲线图报表，柱状图和曲线图报表均支持以数据视图形式展示，柱状图和曲线图报表的查看方式稍有差异，下面分别进行介绍。

### 1) 查看柱状图报表

(a) 将鼠标移动到柱状图上，界面可展示相应类型/节点告警的数量，如下图所示。



(b) 点击柱状图上柱状图形，弹出“报表事件详情”窗口，如下图所示。

报表事件详情							
时间	级别	事件名称	设备地址	源地址	目的地址	一级分类	二级分类
2017-11-14 12:58:39	高	主动日志源异常	127.0.0.1	1.1.1.1	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:57:39	高	主动日志源异常	127.0.0.1	11.11.11.11	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:56:39	高	主动日志源异常	127.0.0.1	10.10.10.10	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:56:39	高	主动日志源异常	127.0.0.1	192.168.25.22	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:53:39	高	主动日志源异常	127.0.0.1	1.1.1.1	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:52:39	高	主动日志源异常	127.0.0.1	11.11.11.11	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:51:39	高	主动日志源异常	127.0.0.1	10.10.10.10	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:51:39	高	主动日志源异常	127.0.0.1	192.168.25.22	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:48:39	高	主动日志源异常	127.0.0.1	1.1.1.1	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:47:39	高	主动日志源异常	127.0.0.1	11.11.11.11	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:46:39	高	主动日志源异常	127.0.0.1	10.10.10.10	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:46:39	高	主动日志源异常	127.0.0.1	192.168.25.22	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:43:39	高	主动日志源异常	127.0.0.1	1.1.1.1	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:42:39	高	主动日志源异常	127.0.0.1	11.11.11.11	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:41:39	高	主动日志源异常	127.0.0.1	10.10.10.10	127.0.0.1	TSM	TopAnalyzer
2017-11-14 12:41:39	高	主动日志源异常	127.0.0.1	192.168.25.22	127.0.0.1	TSM	TopAnalyzer

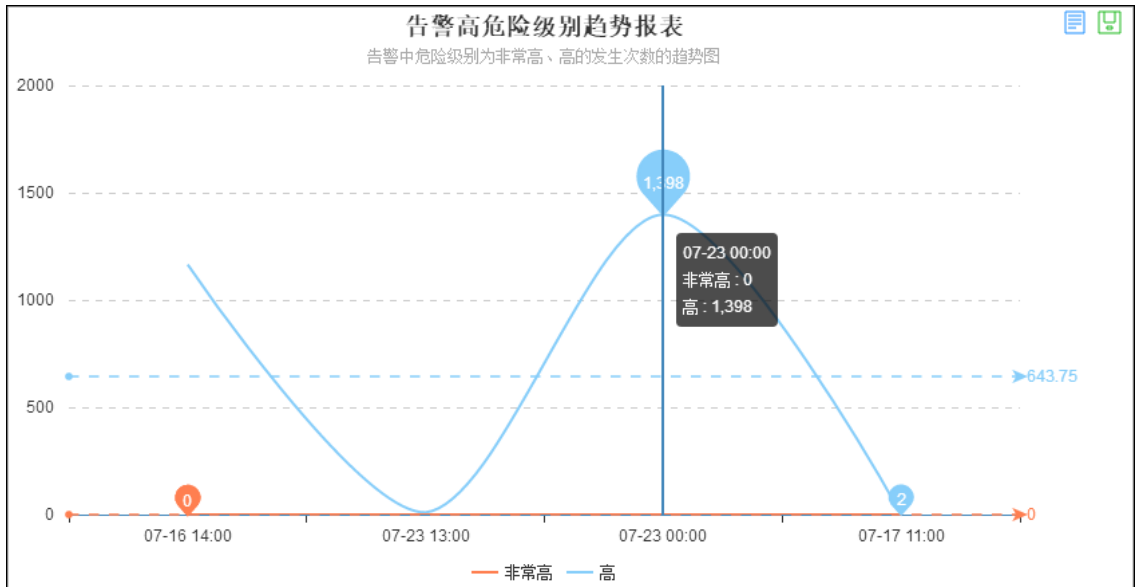
30 | 第 1 共 8 页 | 显示 1 到 30, 共 232 记录

(c) 点击“级别”或“告警名称”字段内容，可下钻到告警查询界面，界面默认展示与该字段内容相关的所有告警信息，关于告警信息的查看请参见 [告警查询](#) (See 5.4.3)。


2) 查看曲线图报表

(a) 告警曲线图以不同颜色的线条标识曲线类型，界面上有明确的说明，如“**非常危险** **高危险**”，其中，实线表示实际的数值，虚线表示平均值。

(b) 将鼠标移动到曲线图上，界面可展示相应时间点相应类型告警的数量，如下图所示。



3) 以数据视图形式展示报表

(a) 点击相应类型报表右上角的数据视图图标“”，报表以列表的形式展示，如下图所示。

告警发生排行  
高频告警发生数

名称	计数
主动日志源异常	198442
节点掉线	5660

关闭

(b) 点击颜色为红色的数据，可下钻到告警查询界面，界面默认展示与该数据相关的所有告警信息。关于告警信息的查看请参见 [告警查询](#)(See 5.4.3)。

### 步骤3 查询、导出报表

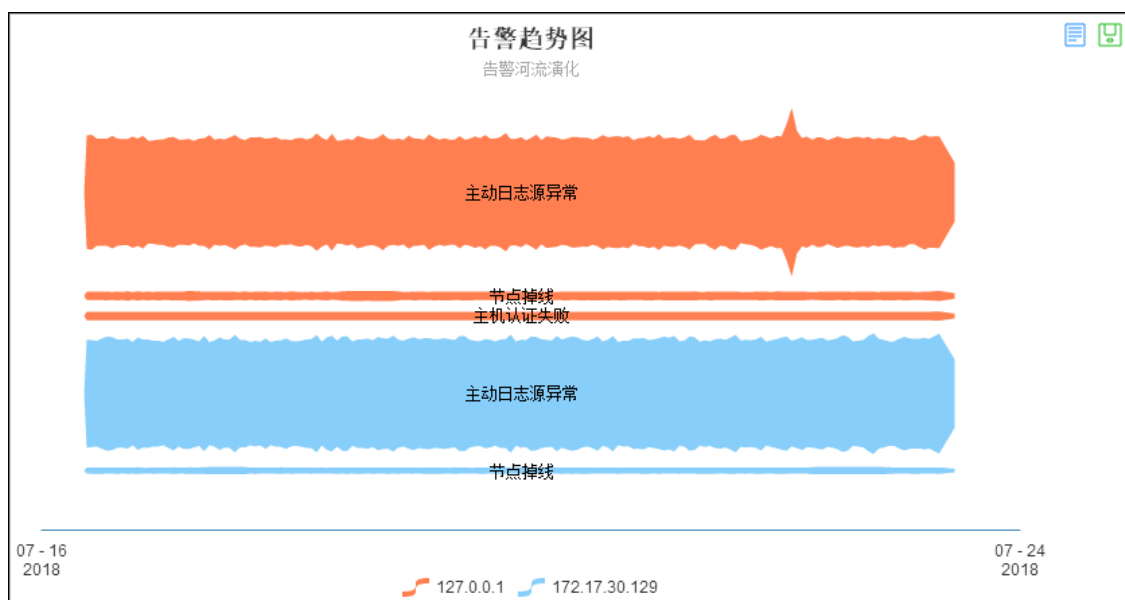
查询和导出告警系列报表的操作方法与系统报表类似，此处不再赘述，关于系统报表的查询和导出操作具体请参见 [系统报表](#)(See 5.3.1.1)。

## 5.3.1.2.2 告警趋势

告警趋势报表界面展示了统计周期内的相应类型告警的数量，以及告警数量随时间的变化趋势。管理告警趋势报表的具体操作步骤如下：

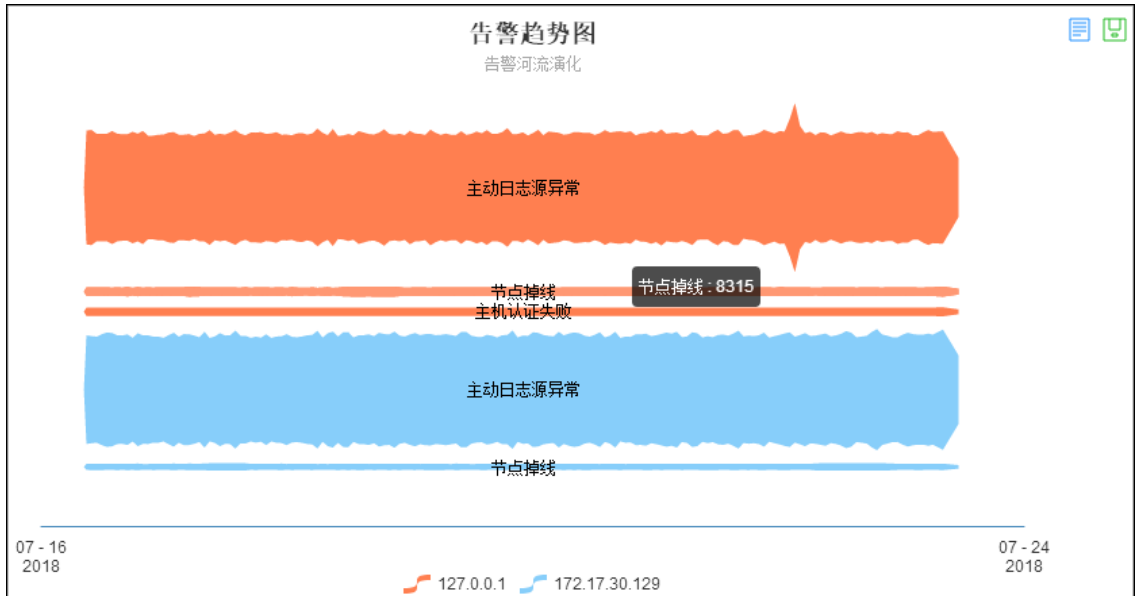
选择 **报表** > **基本报表** > **基础信息报表** > **告警报表** > **告警趋势**，界面默认展示全部节点最近 1 小时整点时间段内的告警趋势报表。如下图所示。

### 步骤1



### 步骤2 查看告警趋势报表

1) 趋势图以不同的颜色曲线标识告警类型/节点，将鼠标移动到趋势图上，界面可展示相应类型告警/节点的数量，如下图所示。



3) 点击相应颜色形状，弹出“报表事件详情”窗口，如下图所示。

报表事件详情							
时间	级别	事件名称	设备地址	源地址	目的地址	一级分类	二级分类
2017-12-06 13:53:31	中	存储上限告警	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer
2017-12-06 13:43:31	中	存储上限告警	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer
2017-12-06 13:33:31	中	存储上限告警	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer
2017-12-06 13:23:31	中	存储上限告警	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer
2017-12-06 13:13:31	中	存储上限告警	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer
2017-12-06 13:03:31	中	存储上限告警	127.0.0.1	127.0.0.1	127.0.0.1	TSM	TopAnalyzer

30 | 第 1 共 1 页 | 显示 1 到 6 共 6 记录

4) 点击“级别”或“事件名称”字段内容，可下钻到告警查询界面，界面默认展示与该字段内容相关的所有告警信息，关于告警信息的查看请参见 [告警查询](#) (See 5.4.3)。

### 步骤 3 查询、导出报表。

查询和导出告警趋势报表的操作方法与系统报表类似，此处不再赘述，关于系统报表的查询和导出操作请参见 [基本报表](#) (See 5.3.1.1)。

---

### 5.3.1.3 日志报表

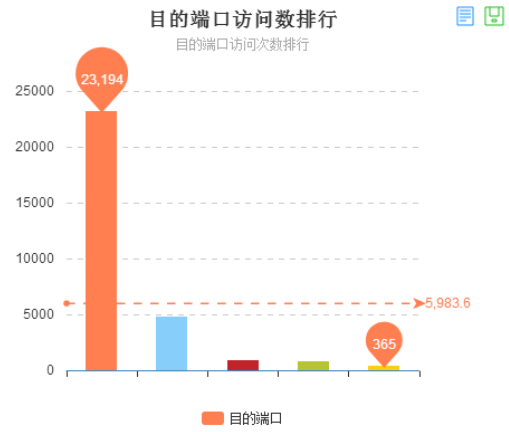
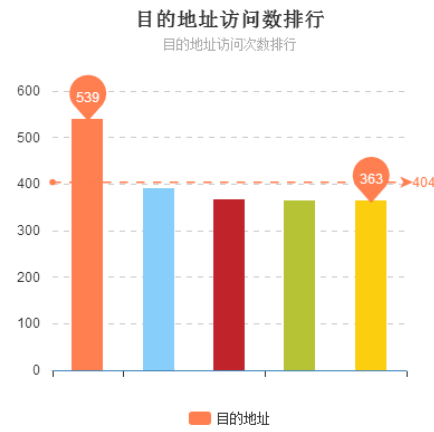
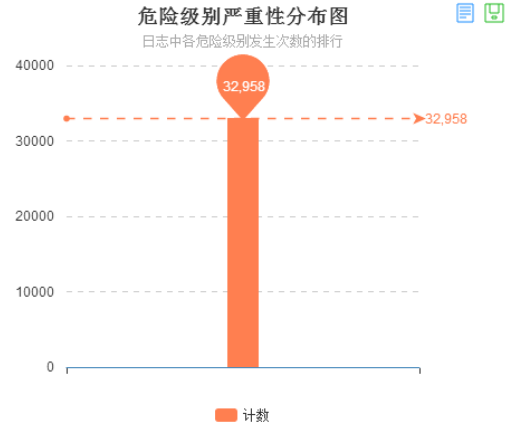
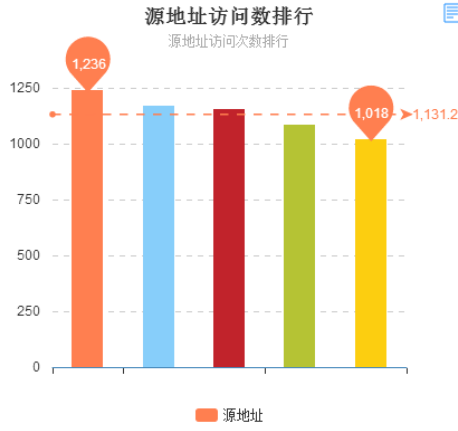
天融信日志收集与分析系统通过对其收集的日志源日志进行提取、分析和统计，形成日志报表，关于日志源的具体介绍请参见 [日志源](#) (See 5.5)。

日志报表界面除了支持展示所有日志源日志概要报表，还支持以日志源设备类型作为分类条件，展示相应类型日志源的日志报表。各种类型的日志报表管理方式类似，下面以“天融信 TOS 防火墙”的“概要报表”为例，介绍管理日志报表的方法。

选择 **报表 > 基本报表 > 基础信息报表 > 日志报表**，点击“天融信 TOS 防火墙”分类下的“概要报表”，界面默认展示全部节点最近 1 小时整点时间段内的报表统计信息。在查看单个节点的报表信息时，报表中会显示平均值、最高数据值和最低数据值，如下

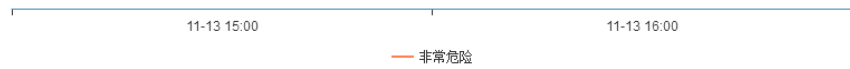
**步骤 1** 图所示。





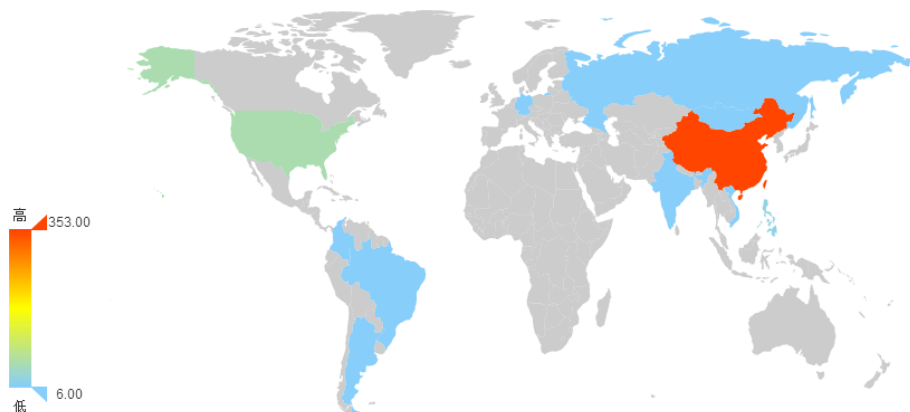
### 高危险级别趋势报表

日志中危险级别为非常高、高的发生次数的趋势图



### 源地址世界分布地图

源地址国家排行



## 步骤 2 查看、查询柱状图报表

查看、查询柱状图日志报表的操作方法与系统报表类似，此处不再赘述，关于系统报表的查看、查询操作请参见 [系统报表](#) (See 5.3.1.1)。

## 步骤 3 查看分布地图报表

分布地图以不同的颜色表示数据的大小，点击地图表示的区域可下钻到日志查询界面，日志查询界面默认展示该区域相关的日志信息，关于日志查询操作请参见 [日志查询](#) (See 5.2.3)。

# 5.3.2 计划报表

计划报表任务即系统根据管理员预先设置的报表生成规则形成报表的任务。当系统时间到达计划报表任务指定的时间时，天融信日志收集与分析系统便触发计划报表任务自动生成报表，并通过邮件将生成的报表发送给指定收件人。

为了适应管理员定制报表的不同需求，天融信日志收集与分析系统计划报表的类型支持天报表、周报表、月报表和年报表；执行时间支持以天、周、月或年为执行周期。



◇不同管理员对计划报表功能模块的操作相对独立，即只有制定该计划报表任务的管理员，才有权限查看以及使用该计划报表任务。

制定计划报表任务及管理生成的报表的具体步骤如下：

**步骤 1** 选择 **报表 > 计划报表**，进入计划报表界面，如下图所示。

名称	类型	用户	导出格式	收件人邮箱	报表类型	下次执行时间	最近编辑时间	状态	操作	下载
report1	基础信息报表	kjh	pdf	kuang@topsec.com.cn	日报表	15日 13时35分	2017-11-14 13:38:37	启用		

## 步骤 2 新建计划报表

1) 在左侧导航树中选择计划报表任务执行周期（每天、每周、每月、每年），然后在右侧界面中点击【新建】按钮，弹出添加计划报表的界面。

2) 设置“计划报表类型”为“基本报表”，便可展开计划报表所有的配置项，如下图所示。

计划报表

**\*名称:**

**\*执行时间:**

**\*计划报表类型:** 基本报表 ▼

---

**\*设备报表主题:**   ▼

**\*已选报表主题:**

**\*时间类型:** 天报表 ▼

**\*数据Top(N):** Top5 ▼

**\*导出文件格式:** pdf文件 ▼

**邮件地址:**   +

**\*已选邮件地址:**-

在新建计划报表时，各项参数的具体说明如下表所示。

参数	说明
名称	设置计划报表的名称。
执行时间	设置系统自动生成报表的执行时间，时间精确到“分”。
计划报表类型	可选项：基本报表。
设备报表主题	选择报表主题及报表需统计的日志所属的日志源。报表主题由系统内置，日志源由管理员添加到系统中，关于日志源的添加请参见 <a href="#">日志源</a> (See 5.5)。
时间类型	设置报表的统计周期，包括：天报表、周报表、月报表、年报表。

参数	说明
	说明： 天报表、周报表、月报表、年报表的统计周期分别为最近一天、最近一周、最近一月、最近一年。
数据 Top(N)	设置对排名前 N 的数据进行统计，可选项包括：Top5、Top10、Top15、Top20、Top25。
导出文件格式	选择报表生成后可导出的报表格式，包括：word 文件、pdf 文件、excel 文件、html 文件。
邮件地址	指定报表收件人的邮箱地址，例如： <a href="mailto:abc@topsec.com.cn">abc@topsec.com.cn</a> 。地址设置完成后，点击“+”，添加邮箱地址，可以添加多个邮箱地址。 说明： 收件人能成功接收到报表的前提条件是：天融信日志收集与分析系统能成功连接到邮件服务器，关于邮件服务器的具体配置请参见 <a href="#">邮件服务器</a> (See 5.7.3.5)。

3) 参数设置完成后，点击页面右下角的【保存】按钮。新建的计划报表可在计划报表列表中显示，管理员可对其进行编辑、删除、禁用和启用操作。




✧新建的计划报表默认是启用状态，管理员可选中计划报表，点击【禁用】按钮禁用计划报表任务。

### 步骤 3 查看执行结果

选择待查看的计划报表任务，点击【执行结果】按钮，可查看计划报表任务的执行情况，如下图所示。

计划报表					
清空		返回			
任务名称	结果	描述	发生时间	执行时长	
1	report1	成功	kuang@topsec.com.cn 计划报表邮件已执行成功	2017年11月14日 13时35分10秒	0.015秒

### 步骤 4 下载计划报表

对于执行成功的计划报表任务，点击“下载”栏的“”，可将生成的报表下载到本地。

## 5.4 告警

天融信日志收集与分析系统提供告警服务，当接收的日志或其自身生成的日志匹配上告警规则，便结合告警规则和告警过滤规则形成告警信息，并根据告警规则定义的告警方式进行报警，关于告警规则和告警过滤规则的具体配置请参见 [告警规则](#) (See 5.7.3.2) 和 [告警过滤规则](#) (See 5.7.3.3)。此外，天融信日志收集与分析系统支持对形成的告警信息进行多维度分析、统计和展示，便于管理员查看各种告警信息，包括告警统计信息、实时告警信息以及历史告警信息。

相关内容包括：

- [告警摘要](#) (See 5.4.1)
- [实时告警](#) (See 5.4.2)
- [告警查询](#) (See 5.4.3)

### 5.4.1 告警摘要

告警摘要界面以告警规则名称、告警级别和日期为统计依据，展示了相应统计时间段内告警的总次数。查看告警摘要的具体操作步骤如下：

选择 **告警 > 告警摘要**，进入告警摘要界面，界面默认展示最近一月的告警摘要信息，

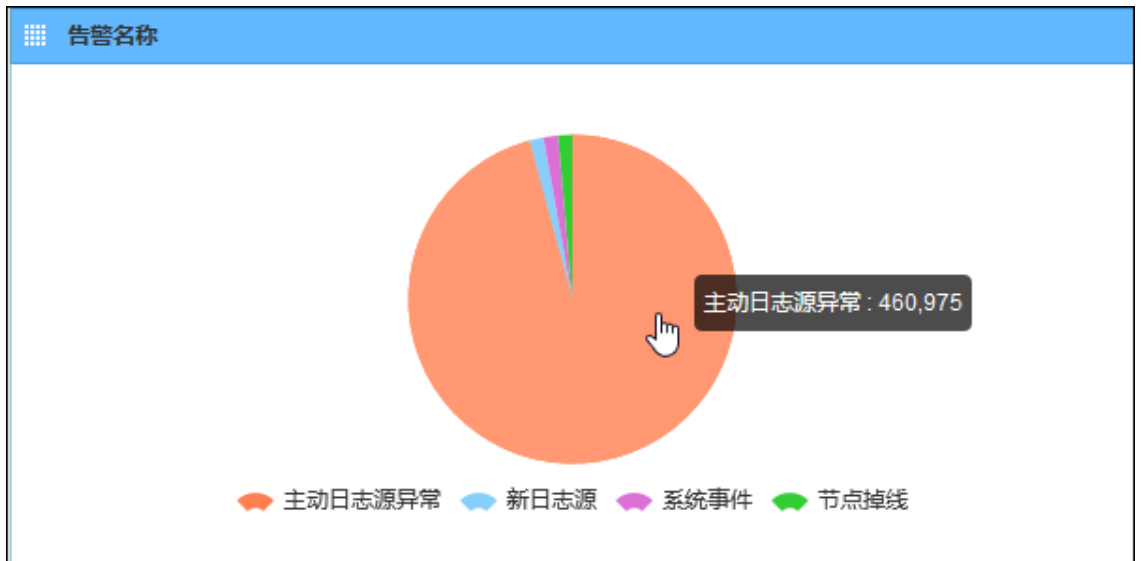
**步骤 1** 如下图所示。



**步骤 2** 查看告警摘要

1) 告警名称维度：以告警名称为视角，通过饼状图的形式显示相应告警规则触发告警的次数。饼状图中以不同的色块区分不同的告警规则。

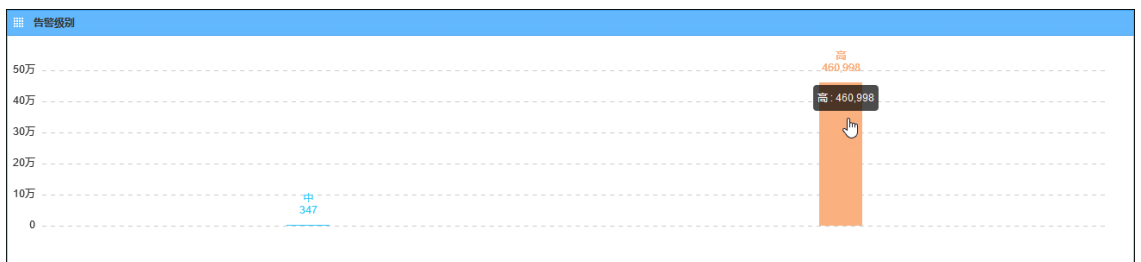
(a) 将鼠标移动到饼状图相应色块上，可展示该色块标识的告警规则触发的所有告警次数，如下图所示。



(b) 点击饼状图色块，可下钻到告警查询界面，界面默认展示该色块标识的告警规则触发的所有告警信息，关于告警信息的查询请参见 [告警查询](#) (See 5.4.3)。

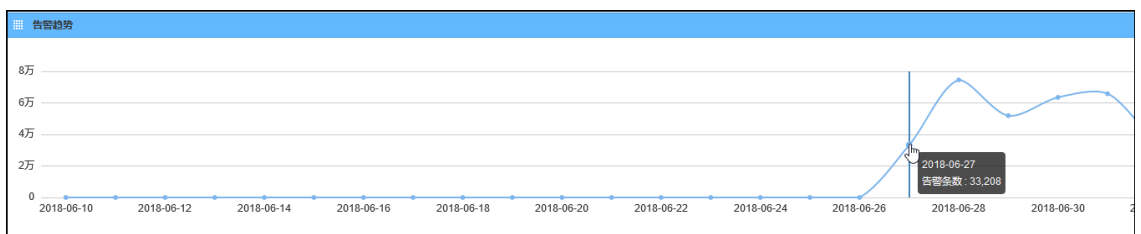
2) 告警级别维度：以告警级别为视角，通过柱状图的形式显示各个级别告警（分为非常低、低、中、高、非常高）的分布情况。

(a) 将鼠标移动到柱状图上，可展示相应告警级别的告警总次数，如下图所示。



(b) 点击柱状图，可下钻到告警查询界面，界面默认展示该柱状图标志的所有告警信息，关于告警信息的查询请参见 [告警查询](#) (See 5.4.3)。

3) 告警趋势：显示告警数量随时间的变化情况。将鼠标移动到曲线图中的节点上，可显示该节点所对应的日期当天的告警总数，如下图所示。



### 步骤 3 查询告警摘要

1) 设置查询条件。

在设置查询条件时，各项参数的具体说明如下表所示。

参数	说明
时间	点击时间控件框，即可进行设置。可选项：最近一小时、最近一天、最近一周、最近一月、今天、昨天、自定义。选择自定义时，可任意设置时间范围。
节点	可选项：全部、127.0.0.1 和节点名称。全部表示本级及下级所有节点；127.0.0.1 表示本级；节点 IP 表示相应节点，关于节点的介绍请参见 <a href="#">节点管理</a> (See 5.7.3.7)。
级别	可选项：全部、非常高、高、中、低、非常低。
告警名称	输入关键字。
源地址	输入源地址。可为 IP 地址的部分内容。
目的地址	输入目的地址。可为 IP 地址的部分内容。



◇ 各个查询字段为逻辑“与”的关系，告警信息所有字段满足设置的查询条件时，才会被统计。

2) 点击【查询】按钮，展示符合条件的告警摘要信息。

#### 步骤 4 导出告警摘要

点击【导出】按钮，可将界面展示的告警摘要信息以 Word 文档的形式导出。

## 5.4.2 实时告警

实时告警界面显示了天融信日志收集与分析系统本级最近的告警信息。管理员可以通过页面左侧的分类（包括告警规则、告警级别）为视角，查看实时告警信息。查看实时告警信息的具体操作步骤如下

步骤 1 选择 **告警 > 实时告警**，进入实时告警监视页面，如下图所示。

时间	告警级别	告警名称	一级分类	二级分类	源地址	目的地址	详情
1 2018-07-11 09:17:58	高	主机日志源异常	TSM	TopAnalyzer	1.1.2.61	127.0.0.1	Systemd类型日志源长时间不发送日志。
2 2018-07-11 09:17:58	高	主机日志源异常	TSM	TopAnalyzer	1.1.1.92	127.0.0.1	Systemd类型日志源长时间不发送日志。
3 2018-07-11 09:17:58	高	主机日志源异常	TSM	TopAnalyzer	1.1.2.66	127.0.0.1	Systemd类型日志源长时间不发送日志。
4 2018-07-11 09:17:58	高	主机日志源异常	TSM	TopAnalyzer	1.1.1.88	127.0.0.1	Systemd类型日志源长时间不发送日志。
5 2018-07-11 09:17:58	高	主机日志源异常	TSM	TopAnalyzer	1.1.2.36	127.0.0.1	Systemd类型日志源长时间不发送日志。
6 2018-07-11 09:17:58	高	主机日志源异常	TSM	TopAnalyzer	1.1.2.50	127.0.0.1	Systemd类型日志源长时间不发送日志。

实时告警包括告警规则和告警级别，如下图所示。

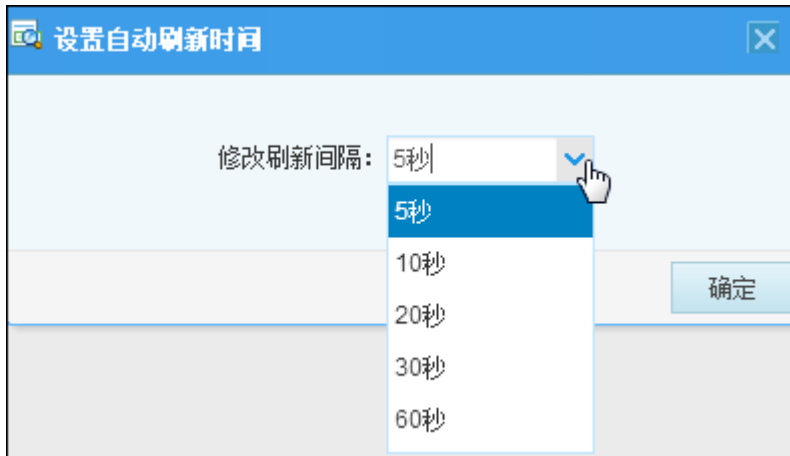
告警规则	时间	告警级别	告警名称	一级分类	二级分类	源地址	目的地址	详情
新日志源	1 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.169	127.0.0.1	System:主动日志源长时间不发送日志。
节点离线	2 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.253	127.0.0.1	System:主动日志源长时间不发送日志。
主站日志源异常	3 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.186	127.0.0.1	System:主动日志源长时间不发送日志。
存储已上电	4 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.235	127.0.0.1	System:主动日志源长时间不发送日志。
存储上报告警	5 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.113	127.0.0.1	System:主动日志源长时间不发送日志。
资产编成	6 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.168	127.0.0.1	System:主动日志源长时间不发送日志。
日志定时不发送	7 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.126	127.0.0.1	System:主动日志源长时间不发送日志。
主机认证失败	8 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.125	127.0.0.1	System:主动日志源长时间不发送日志。
用户策略能力破解失败	9 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.124	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	10 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.236	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	11 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.127	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	12 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.122	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	13 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.121	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	14 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.120	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	15 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.137	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	16 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.136	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	17 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.135	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	18 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.134	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	19 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.139	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	20 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.138	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	21 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.133	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	22 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.132	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	23 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.128	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	24 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.131	127.0.0.1	System:主动日志源长时间不发送日志。
应用程序策略用户策略能力	25 2018-07-11 10:30:58	严重	主动日志源异常	TSM	TopAnalyzer	1.1.130	127.0.0.1	System:主动日志源长时间不发送日志。

告警规则类型主要分为系统内置和自定义，关于告警规则配置请参见[告警规则](#)。(See 5.7.3.2)

设置告警级别，可选择查询条件为非常高、高、中、低、非常低。

### 步骤 2 设置刷新间隔

1) 点击告警监视列表上方的【刷新闻隔】按钮，弹出“设置自动刷新时间”对话框，通过下拉列表选择时间（可选项：5 秒、10 秒、20 秒、30 秒、60 秒），如下图所示。



2) 点击【确定】按钮，系统便根据设置的刷新间隔自动刷新实时告警信息。

### 步骤 3 启用/停止自动刷新实时告警信息

点击告警列表上方的【停止刷新】按钮，可以停止自动刷新实时告警信息，此时【停止刷新】按钮切换为【启动刷新】，点击【启动刷新】按钮，可启动自动刷新实时告警信息功能。

### 步骤 4 清空实时告警信息

点击【清空】按钮，可以将界面中显示的所有告警信息删除。



## 5.4.3 告警查询

天融信日志收集与分析系统支持以多种角度对告警信息进行查询，包括：触发告警的告警规则名称、告警级别、告警信息产生时间、告警节点以及告警信息的地址。查询告警规则的具体操作步骤如下：

**步骤 1** 选择 **告警 > 告警查询**，进入告警查询界面，如下图所示。



**步骤 2** 查看告警信息

1) 点击告警列表中的“级别”字段或带下划线的字段内容，如告警级别、告警名称、节点、源地址、目的地址、设备地址等，系统则在当前界面中查询条件的基础上，再将该字段的内容作为查询条件，筛选出与查询条件匹配的所有告警信息。如下图所示。



2) 点击告警列表的“关联日志”字段内容，界面下方展示触发该告警的日志信息，如下图所示。

级别	类型	事件名	源地址	目的地址	操作
中	SysEvent	目标主机认证失败	172.17.30.130	172.19.8.14	asset_auth_failed

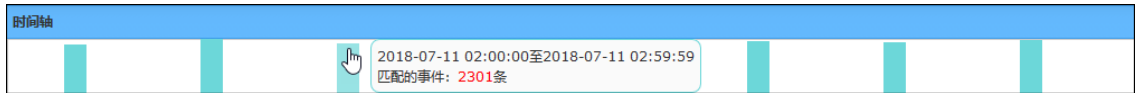
3) 点击“源地址”/“目的地址”字段的查看日志图标“📄”，系统将该源地址/目的地址作为查询条件，展示该源地址/目的地址相关的所有日志信息，关于日志的查看请参见 [日志查询](#) (See 5.2.3)。

4) 点击告警列表“源地址”/“目的地址”字段的访问树图标“🌳”，进入源地址/

目的地址访问次数统计界面，点击访问次数统计界面左上角的设置图标“⚙️”，可设置访问树查询条件。

**步骤 3** 查看时间轴

时间轴以柱状图显示统计周期内的告警总数，将鼠标移动到柱状图图形上，展示相应时间段内的告警总数，如下图所示。



如果告警查询界面设置的时间统计周期不超过 3 天（最近一小时、最近一天、今天、昨天、自定义三天内的时间），时间轴以每小时为单位，展示每小时时间内的告警总数；否则，时间轴以天为单位，展示相应日期当天的告警总数。

#### 步骤 4 查询告警信息

- 1) 在左侧“告警查询”导航树中选择规则名称或告警级别，然后在右侧“告警查询列表”区域设置查询条件。
- 2) 点击【查询】按钮，符合条件的告警信息将被筛选出来。

#### 步骤 5 点击【导出】按钮，可将界面展示的告警信息以压缩包方式导出到本地。

## 5.5 日志源

日志源管理模块可集中管理所有的日志源，用户可以通过此模块方便地查看系统配置的所有日志源相关信息并进行管理。日志源分为两类：一类可以主动向系统发送日志，称为主动型日志源；另外一类日志源称为被动型日志源，这类日志源不主动向系统发送日志，需要通过收集代理去收集。同时，系统提供了业务组功能，用户可用此功能将日志源分组，在日志查询统计时便于审计分析。

相关内容主要包括：

- [日志源管理](#) (See 5.5.1)
- [业务组](#) (See 5.5.2)

### 5.5.1 日志源管理

操作管理员在日志源管理功能中可以查看日志源的名称、IP 地址、类型、收集节点、所属业务组等信息，也可以进行新建、编辑、启用/禁用、删除和查询等操作。日志源管理的具体操作步骤如下：

#### 步骤 1 选择 日志源 > 日志源管理，进入日志源管理界面，如下图所示。

日志源名称	IP地址	日志源类型	收集节点	业务组	收集方式	最近接收时间	今日日志趋势	重置日志时间	日志保存时间	报表保存时间	状态	操作
192.168.75.10	192.168.75.10	天融信TOS防火墙	127.0.0.1	123	Syslog	2017-12-06 13:38:13			6个月	6个月	启用	
172.19.21.72	172.19.21.72	微软Windows系列服务器	127.0.0.1	123	WMI	2017-12-06 13:36:00			6个月	6个月	启用	
172.19.8.11	172.19.8.11	通用Syslog设备	192.168.75.10		Syslog	2017-11-13 09:52:41	-		6个月	6个月	禁用	
test	1.2.5.8	SqlServer系统日志	192.168.75.10		TXT	2017-11-09 10:34:05	-		6个月	6个月	禁用	
1.2.3.6	1.2.3.6	天融信TopFlow	192.168.75.10		Syslog	2017-12-06 13:43:14			6个月	6个月	启用	
1.2.3.7	1.2.3.7	天融信WEB应用防火墙	192.168.75.10		Syslog	2017-12-06 13:43:12	-		6个月	6个月	启用	
WSA	192.168.75.10	H3C透传防火墙	192.168.75.10		Syslog	2017-11-22 10:47:51	-		6个月	6个月	启用	

#### 步骤 2 新建

- 1) 点击【新建】按钮，进入新建日志源界面，如下图所示。

\*日志源名称：8.14 ✓

\*日志源IP：172.19.8.14 ✓

\*日志源类型：微软Windows系列服务器 ?

\*收集节点：127.0.0.1 ?

\*收集方式：WMI ✓

日志源状态： 启用

存储原始日志：是

覆盖日志时间：否

轮询时间：分钟间隔 1 分

日志保存：6 个月

报表保存：6 个月

过滤规则：请选择 ?

业务组：

\*加密密码：否

\*用户名：

\*密码：

界面中各参数的说明请参见下表。

参数	说明
日志源名称	必填项。设定日志源名称。
日志源 IP	必填项。填写日志源的设备或系统的 IP 地址。 TA-L 支持批量添加日志源。批量添加日志源时，日志源 IP 之间使用英文逗号分隔，创建完成的日志源名称为“日志源 IP”+“日志源名称”。即此时“日志源名称”文本框中的内容为日志源名称的后缀。 例：日志源名称输入“abc”，日志源 IP 输入 1.1.1.1,2.2.2.2，那么这两个日志源名称分别为 1.1.1.1abc 和 2.2.2.2abc。

参数	说明
日志源类型	必填项。通过下拉列表选项日志源设备的类型。
收集节点	必填项。针对主动型日志源，此处填写 127.0.0.1；针对被动型日志源，此处填写代理服务器 IP 地址。 说明： 支持用户手动输入，并可进行快速过滤，帮助用户实现智能输入。
收集方式	必填项。不同的日志源有不同的收集方式供用户选择，主要有 TXT、SFTP、Syslog、FTP、NewFlow 等。
日志源状态	是否启用该日志源。
存储原始日志	通过下拉列表选择是否存储原始日志。
覆盖日志时间	是否以接收日志的天融信日志收集与分析系统的系统时间覆盖日志在日志源设备中的发生时间，默认为“否”。
活跃度	超过“活跃度”时间后，如果主动型日志源不向 TA-L 系统发送日志，TA-L 系统会自动产生“主动日志源异常”告警，并且之后每 5 分钟产生一次“主动日志源异常”告警，直到该日志源主动向 TA-L 系统发送日志为止。关于“主动日志源异常”告警的查看请参见 <a href="#">告警</a> (See 5.4)。 说明：仅在添加主动型日志源时，需配置该参数。
限速	限制 TA-L 系统收集该日志源日志的速度，超过限速的日志将会被丢弃，单位：条/秒。 说明：仅在添加主动型日志源时，需配置该参数。
日志保存	日志源设备传输到天融信日志收集与分析系统中的日志数据的保存时间。 在下拉框中选择，可选项有：1 个月、2 个月、3 个月、6 个月、12 个月以及永远。
报表保存	设置日志源相应的报表数据的保存时间，超过设定时间的报表数据将会删除。
过滤规则	从下拉列表选择一个过滤规则，日志源类型与过滤规则必须匹配设置，具体规则说明请参见 <a href="#">日志过滤规则</a> (See 5.7.3.1)。
业务组	设备有下级节点时，需设置该参数，选择该日志源所属的业务组，方便管理员进行管理。关于业务组的配置具体请参见 <a href="#">业务组</a> (See 5.5.2)。

参数	说明
编码	设置日志的编码格式。
加密密码	设置进行日志外发时，日志的加密密码。
用户名	设置指定 IP 地址的登录用户名。
密码	设置指定 IP 地址的登录用户名对应的密码。


以上为日志源基本设置项。不同的日志源类型，还会增加用户名与密码等其他配置项。



✦对 snmp、syslog、netflow 类型日志源增加了限制，即这三种收集方式不允许存在重复 IP 的日志源。  
 ✦当日志源类型是“天融信 TOS 防火墙”，需要将日志进行加密外发时，需设置“加密密码”参数，该参数的值跟防火墙外发配置中的“加密密码”值一样。

2) 参数设置完成后，点击【保存】按钮。

### 步骤 3 编辑

1) 在日志源列表中选择需要修改的日志源，点击编辑图标“”，进入日志源编辑页面，如下图所示。

*日志源名称 :	8.14	✓
*日志源IP :	172.19.8.14	✓
*日志源类型 :	微软Windows系列服务器	?
*收集节点 :	127.0.0.1	?
*收集方式 :	WMI	✓
日志源状态 :	<input checked="" type="checkbox"/> 启用	
存储原始日志 :	是	
覆盖日志时间 :	否	
轮询时间 :	分钟间隔 1 分	
日志保存 :	6 个月	
报表保存 :	6 个月	
过滤规则 :	请选择	?
业务组 :		
*加密密码 :	否	
*用户名 :		
*密码 :		

2) 编辑完成后, 点击“保存”按钮即可。


#### 步骤 4 批量修改

相同类型的日志源可以同时选中, 点击【批量修改】按钮进行批量修改。


#### 步骤 5 启用/禁用

在日志源列表中选择日志源, 点击【启用】或【禁用】按钮即可对日志源设备进行启用或禁用操作。选中多条数据也可以进行批量操作。

#### 步骤 6 删除

在日志源列表中选择需要删除的日志源, 点击删除图标“”, 弹出确认删除提示框, 点击【确定】按钮即可将日志源删除, 点击【取消】按钮取消删除操作。

#### 步骤 7 查询

界面中显示已有的日志源列表，操作管理员可以在列表上方设置查询字段信息，包括：日志源名称、日志源 IP、日志源类型、收集节点、业务组，点击“”可以展开状态、创建者两个查询条件，设置完成后点击【查询】按钮即可列出查询结果。点击【清空】按钮即可清空设置条件。

#### 步骤 8 其他

点击【配置列】按钮，可设定显示在查询结果列表中的字段。

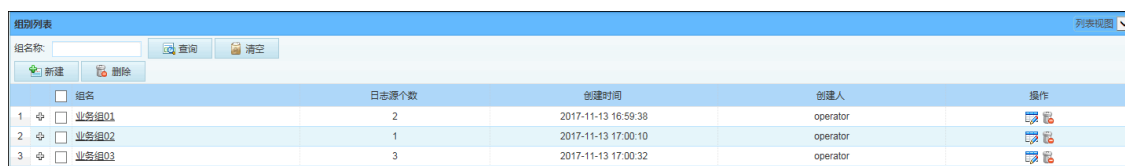
点击列表中相应数据的“日志源名称”字段，可下钻到系统日志查询界面，界面默认展示与该日志源相关的日志信息，关于系统日志查询请参见 [日志查询](#) (See 5.2.3)。

移动光标至相应数据的“今日日志趋势”字段，可显示自凌晨至当前时间段内不同时间点的日志数量。

## 5.5.2 业务组

业务组功能可将类型、用途等相同的本级或下级日志源归为一组，方便操作管理员根据业务组查看日志（相关查询操作请参考 [日志查询](#) (See 5.2.3)）。只有预置操作管理员可以对业务组进行管理，自定义操作管理员无业务组功能菜单的操作权限，也不能在日志查询模块以业务组角度查看统计信息，但在主页的“系统拓扑”页面以业务组的方式查看系统的拓扑情况。业务组管理的具体操作步骤如下：

**步骤 1** 选择 **日志源 > 业务组**，如下图所示。



截图显示了一个名为“组列表”的界面。顶部有一个搜索框，旁边有“查询”和“清空”按钮。下方有“新建”和“删除”按钮。表格列出了三个业务组：

组名	日志源个数	创建时间	创建人	操作
1 <input type="checkbox"/> 业务组01	2	2017-11-13 16:59:38	operator	
2 <input type="checkbox"/> 业务组02	1	2017-11-13 17:00:10	operator	
3 <input type="checkbox"/> 业务组03	3	2017-11-13 17:00:32	operator	


#### 步骤 2 新建

1) 点击【新建】按钮，弹出“创建业务组”窗口，如下图所示。




2) 输入业务组的名称，选择需要关联的日志源，点击【保存】按钮即可。

### 步骤 3 编辑



在业务组列表中选择需要修改的业务组，点击相应操作栏中的编辑图标“”，进入业务组修改页面，修改完成后点击【保存】即可。

### 步骤 4 删除

在业务组列表中选择需要删除的业务组，点击删除图标“”，弹出确认删除提示框，点击【确定】按钮即可将业务组删除，点击【取消】按钮取消删除操作。

### 步骤 5 查询

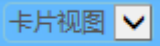
设置“组名称”后点击【查询】按钮即可得到查询结果。

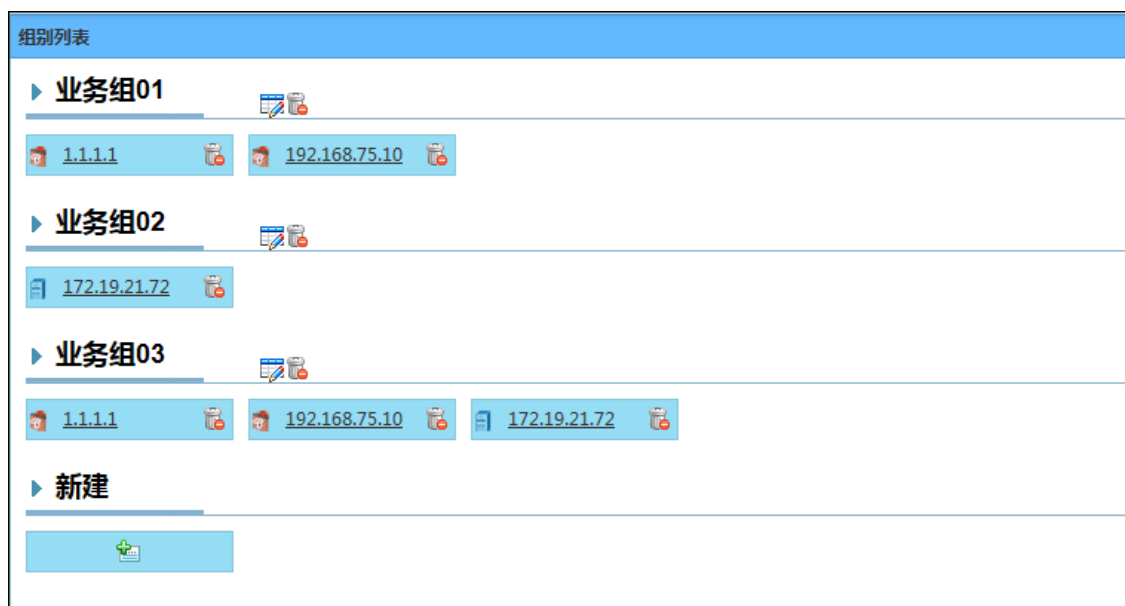
点击某条业务组前面的加号图标“”，可展开该业务组包含的日志源名称、IP 地址等信息。点击“日志源名称”字段，可下钻到日志查询界面，界面默认展示与该日志源相关的日志信息，关于日志查询请参见 [日志查询](#)(See 5.2.3)。点击减号图标“”，即

步骤 6 可关闭展示信息。

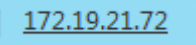
步骤 7 卡片视图



选择视图下拉列表框中的卡片视图，如图“”，可切换为卡片视图展示。如下图所示。



1) 该视图中所示图标操作与列表视图类似：新建操作请参考 [步骤 2](#) (See 5.5.2)，编辑操作请参考 [步骤 3](#) (See 5.5.2)，删除操作请参考 [步骤 4](#) (See 5.5.2)。

2) 点击日志源字段，如图“”，可下钻到日志查询界面，界面默认展示与该日志源相关的日志信息，关于日志查询请参见 [日志查询](#) (See 5.2.3)。

## 5.6 知识库

天融信日志收集与分析系统（企业版）的知识库模块提供了一定的规则对知识进行分类管理，使知识有序化。并提供检索功能，为有效使用打下了基础。已经添加的知识可用于告警规则配置，关联二者后，匹配该告警规则产生的告警信息，用户可以在“告警查询”列表中查看该告警信息所关联知识的解决方法。知识库管理的具体操作步骤如下：

**步骤 1** 选择 **知识库 > 知识库**，进入知识库管理页面。页面左侧为知识组织架构，右侧是知识列表信息。如下图所示：

名称	时间	一级分类	二级分类	创建人	描述	操作
<input type="checkbox"/> CG代理	2017-12-11 15:17:42	网络攻击	CG攻击	operator	CG代理是Common Gateway Interface (公用网关接口) 的简称，并不特指一种类型。CG代理是服务器和客户端之间的桥梁，它接收客户端的请求，并将请求转发给服务器。CG代理还可以提供缓存、负载均衡、使用请求等功能。	
<input type="checkbox"/> 通信故障或数据已丢失	2017-12-11 16:11:27	系统故障	通信故障	tt	提示通信故障或数据已丢失	
<input type="checkbox"/> windows无法启动通信窗口	2017-12-11 16:10:59	系统故障	通信故障	tt	windows无法启动通信窗口	
<input type="checkbox"/> 口令攻击	2017-12-11 16:15:28	网络攻击	口令猜测	operator	1 攻击者利用各种工具或脚本程序对口令进行攻击，并不特指一种类型。攻击者通过猜测或暴力破解等方式，获取系统管理员或普通用户的口令。如果攻击者成功获取了口令，就可以获得系统管理员或普通用户的权限。攻击者还可以通过猜测或暴力破解等方式，获取系统管理员或普通用户的口令。攻击者还可以通过猜测或暴力破解等方式，获取系统管理员或普通用户的口令。	
<input type="checkbox"/> 后门攻击	2017-12-11 16:22:26	网络攻击	后门攻击	operator	在信息安全领域，后门是指绕过安全防护机制对程序或系统漏洞的访问。后门的主要目的是绕过安全防护机制，从而实现对系统或数据的非法访问。攻击者可以通过后门攻击，获取系统管理员或普通用户的权限。攻击者还可以通过后门攻击，获取系统管理员或普通用户的口令。	
<input type="checkbox"/> 域名劫持	2017-12-11 16:25:41	网络攻击	域名劫持	operator	域名劫持是指攻击者通过非法手段，将目标网站的域名解析到攻击者控制的服务器上。攻击者可以通过域名劫持，获取目标网站的流量。攻击者还可以通过域名劫持，获取目标网站的敏感信息。	
<input type="checkbox"/> 扫描探测	2017-12-11 16:37:42	网络攻击	扫描探测	operator	扫描探测是指攻击者通过扫描探测工具，对目标系统进行扫描探测。攻击者可以通过扫描探测，获取目标系统的漏洞信息。攻击者还可以通过扫描探测，获取目标系统的敏感信息。	

**步骤 2** 点击【新建】按钮，即可新建知识。填写完成后点击【保存】按钮即可。如下图所示：

The image shows a '新建' (New) dialog box with the following fields and controls:

- 名称** (Name): A text input field with a cursor.
- 一级分类** (Primary Classification): A dropdown menu.
- 二级分类** (Secondary Classification): A dropdown menu.
- 描述** (Description): A large text area.
- 解决方法** (Solution Method): A large text area.
- 保存** (Save) and **取消** (Cancel): Two buttons at the bottom right.


各项参数的具体说明如下表所示。

参数	说明
名称	必填项。定义知识的名称。
一级分类	必填项。一级分类包含：信息破坏、内容安全、可疑异常、有害程序、状态信息、系统审核、系统故障、网络审计、网络攻击、计费、TSM。
二级分类	必填项。二级分类由以上一级分类级联显示。
描述	选填项，填写相关描述信息。
解决方法	选填项，填写相关的解决方法。

点击某条需要修改的知识对应的编辑图标“”，进入“编辑”页面修改，完成后点

**步骤 3** 击【保存】按钮即可。

点击某条知识前面的加号图标“”，可展开“解决方法”的信息；点击减号图标

**步骤 4** “”，即可关闭展示信息。

**步骤 5** 选中某条要删除的知识，点击知识列表上方的【删除】按钮即可完成操作。

**步骤 6** 在条件输入框中输入知识的“名称”后，点击【查询】便可查询相应的知识信息。

## 5.7 配置

配置模块相关内容包括：

- [存储管理](#) (See 5.7.1)：设置日志的存储策略和备份策略。
- [转发配置](#) (See 5.7.2)：设置 Syslog 和 JMS 的转发配置。
- [系统配置](#) (See 5.7.3)：对日志收集与分析系统进行日志过滤、告警、节点管理、系统备份等操作。

### 5.7.1 存储管理

通过存储管理模块，可以设置日志存储策略和备份策略。

#### 5.7.1.1 存储策略

日志存储策略主要用来设置日志存储的路径，处理历史日志对系统磁盘的影响。其设置步骤如下：

**步骤 1** 选择 **配置 > 存储管理 > 存储策略**，进入日志存储策略设置页面，如下图所示。

### 日志存储策略的配置

描述 日志存储策略的配置

日志存储路径

\*当前存储路径

\*磁盘使用率(%)

\*磁盘使用率告警上限(%)

启用保护  启用

参数说明见下表：

参数	说明
日志存储路径	<p>设置日志的存储路径，由于存储日志需要大量磁盘空间，所以需要配置到大容量硬盘分区上。日志存储路径不能与备份路径在同一磁盘分区上。不支持中文路径。</p> <p>说明：</p> <p>可以设置多条存储路径，防止日志溢出。即在“当前存储路径”的磁盘存储达到规则上限后会自动跳转到下一个存储路径，管理员也可手动修改“当前存储路径”为存储路径中的其他路径。但是需在日志存储路径中保留原来的“当前存储路径”，以免造成日志信息丢失。</p>
当前存储路径	<p>设置日志当前存储路径，由于存储日志需要大量磁盘空间，所以需要配置到大容量硬盘分区上。</p> <p>说明：</p> <p>“当前存储路径”是“日志存储路径”中的一个。默认路径是安装时指定的路径。</p>
磁盘使用率（%）	<p>设置存储路径所在的磁盘分区使用率。超过此阈值时，将会删除最早的外部日志，请慎重操作。</p>
磁盘使用率告警上限（%）	<p>设置存储路径所在的磁盘分区使用率的告警上限。超过此使用率时，会产生告警。</p>
启用保护	<p>启用保护后，设置的所有存储路径被保护起来，存储路径下的文件不允许被服务器进程以外的其他进程删除和修改。如果无法启动保护机制，请确认在安装本系统时 TopDesk_X64 程序是否安装成功。</p>

**步骤 2** 参数配置完成后，点击【应用】按钮即可。

## 5.7.1.2 备份策略

**步骤 1** 选择 **配置 > 存储管理 > 备份策略**，进入备份策略设置页面。

系统支持两种备份方式：本地备份和 FTP 备份。本地备份是指将日志文件备份到 TA-L 系统服务器上；FTP 备份则是指将日志文件备份到 FTP 服务器上。

➤ 本地备份

### 日志备份策略配置

**描述** 日志备份配置，专业人员使用。

备份方式  本地备份  FTP备份

\*本地备份路径

备份范围

保留告警天数

是否启用  启用

当选择本地备份时，需要设置本地备份路径（注意备份路径不能与日志存储路径在同一磁盘分区）、备份范围、备份文件保留的时间等参数。

➤ FTP 备份

日志备份策略配置

**描述** 日志备份配置，专业人员使用。

备份方式  本地备份  FTP备份

\*服务器IP地址

\*用户名

\*口令

编码

备份范围

保留告警天数

是否启用  启用

当选择备份到 FTP 服务器上时，需设置 FTP 服务器地址、用户名、密码、编码、备份范围、备份文件保留时间等参数。

参数说明见下表：

参数	说明
服务器 IP 地址	设置备份日志的服务器的 IP 地址。
用户名	设置登录备份日志的服务器的用户名。
口令	设置登录备份日志的服务器的口令。
编码	设置备份日志所使用的编码。可选项：GB2312、UTF-8。
备份范围	设置自动备份的周期。可选项有：1 个月前、2 个月前、3 个月前、4 个月前、5 个月前、6 个月前和一年前。 备份范围是指从当前备份时间开始向前推算。例如：设置备份范围为 1 个月前，系统将自动备份一个月前的所有日志。

---

参数	说明
是否启用	设置是否启用该自动备份策略。
保留告警天数	设置告警在备份服务器数据库中保留的天数。默认保留 6 个月。

**步骤 2** 备份参数设置完成后，点击【应用】按钮即可。

## 5.7.2 转发配置

通过转发配置模块，可以设置 Syslog 日志和 JMS 日志的转发规则。

### 5.7.2.1 Syslog 转发

系统支持日志转发功能，可以把收集到的日志以 syslog 形式转发到指定地址。

选择 **配置 > 转发配置 > Syslog 转发**，进入“Syslog 日志转发配置”页面。如下图所示。  
**步骤 1** 示。

**Syslog日志转发配置**

**描述** 将日志进行格式化后，以syslog方式转发给需要的设备。

### Syslog日志转发配置

\*日志转发IP地址

\*端口

\*发送最大频率

状态  启用

仅转发原始日志  是

发送JSON格式  是

\*过滤器  默认  
编辑

### 日志转发头信息设置

头信息分隔符

头信息前缀

是否包含设备IP地址  是

应用

参数说明见下表：

参数	说明
日志转发 IP 地址	设置日志转发目的 IP 地址。多个地址使用逗号分隔。
端口	设置转发端口，默认端口 514。
发送最大频率	设置每秒钟转发日志的最大条数，范围：0-5000。
状态	设置是否转发 Syslog 日志。
仅转发原始日志	设置是否只转发原始日志。勾选表示只转发原始日志；不勾选表示转发所有日志。



参数	说明
发送 JSON 格式	设置是否以 JSON 格式发送日志。勾选表示以 JSON 格式发送日志，此时，不需要进行日志转发头信息设置。
过滤器	设置要转发的日志的过滤条件。 可以点击“默认”按钮选择默认的过滤条件，也可以选择点击“编辑”按钮，在弹出的条件编辑对话框中编辑过滤条件。过滤条件编辑好后，依次点击“插入”、“验证”，验证成功后点击“完成”方可使过滤规则创建成功。
头信息分隔符	用于区分头信息。
头信息前缀	信息分隔字符，例如" "。
是否包含设备 IP 地址	设置日志转发头包含设备的 IP 信息，勾选后头信息包含设备地址 IP。

**步骤 2** 参数配置完成后，点击【应用】按钮即可。

## 5.7.2.2 JMS 转发

系统支持日志转发功能，可以把系统收集到的日志以 JMS 形式转发到指定的服务器上。

**步骤 1** 选择 **配置 > 转发配置 > JMS 转发**，进入“JMS 日志转发配置”页面。如下图所示。

**描述** 将日志进行格式化后以JMS方式转发给需要的设备。

\*日志转发IP地址

\*端口

\*Topic

用户

密码

\*加密  是  否

\*发送最大频率

\*转发状态  启用

\*过滤器  默认  
编辑

参数说明见下表：

参数	说明
日志转发 ip 地址	设置接收 JMS 日志的服务器的 IP 地址。只支持一个。
端口	设置转发端口，默认端口 61616。
Topic	设置 JMS 消息的 Topic。
用户	接收日志的服务器的用户名。
密码	接收日志的服务器的用户名对应的密码。
加密	设置转发时是否加密。
发送最大频率	设置每秒钟转发日志的最大条数，范围：0-5000。
转发状态	设置是否转发 JMS 日志。

参数	说明
过滤器	<p>设置要转发的 JMS 日志的过滤条件。</p> <p>可以点击“默认”按钮选择默认的过滤条件，也可以选择点击“编辑”按钮，在弹出的条件编辑对话框中编辑过滤条件。过滤条件编辑好后，依次点击“插入”、“验证”，验证成功后点击“完成”方可使过滤规则创建成功。</p>

**步骤 2** 参数配置完成后，点击【应用】按钮即可。

## 5.7.3 系统配置


系统配置主要包括日志过滤规则配置、告警规则配置、邮件服务器配置、采集器端口、告警方式管理、代理管理、服务器升级、代理升级、系统备份等，下面将分别加以介绍。

### 5.7.3.1 日志过滤规则

设置日志过滤规则。规则创建后需被日志源引用才能生效，日志源引用规则操作请参见 [日志源管理](#) (See 5.5.1)。

**步骤 1** 选择 **配置 > 系统配置 > 日志过滤规则**，进入过滤规则页面，如下图所示。



**步骤 2** 点击列表上方的“”新建，进入新建页面，如下图所示。

**日志过滤规则配置**

**描述** 日志源将保留或丢弃符合过滤规则的信息。

**\*过滤器名称**

**\*日志源类型**

**过滤模式**  保留模式  丢弃模式

**是否启用**  启用

**\*过滤器**

默认

编辑

参数说明见下表：

参数	说明
过滤器名称	定义一个过滤器的名称。
日志源类型	通过下拉列表选择需要过滤的日志源。
过滤模式	分为“保留模式”和“丢弃模式”。“保留模式”是指保留符合过滤条件的日志；“丢弃模式”丢弃符合过滤条件的日志。
是否启用	确定是否启用此过滤规则应用于选定的日志源。
过滤器	设置日志的过滤条件。 可以点击“默认”按钮选择默认的过滤条件，也可以选择点击“编辑”按钮，在弹出的条件编辑对话框中编辑过滤条件。过滤条件编辑好后，依次点击“插入”、“验证”，验证成功后点击“完成”方可使过滤规则创建成功。

**步骤 3** 设置完成后点击【保存】，系统自动刷新页面返回至过滤规则列表页面。

**步骤 4** 点击某个规则所在行的“”编辑，进入编辑页面进行修改，完成后点击【保存】即

可。

通过点击规则名称前的复选框选择一个或多个规则后，点击“”启用或“”禁用

**步骤 5** 完成告警的启停操作。

通过点击规则名称前的复选框选择一个或多个规则后，点击“”删除，在出现的对话框

**步骤 6** 框进行确认即可。

**步骤 7** 通过设置规则名称、状态、日志源类型，点击【查询】可以查询日志过滤规则。

## 5.7.3.2 告警规则

告警规则主要用于配置告警规则属性、关联条件。

**步骤 1** 选择 **配置 > 系统配置 > 告警规则**，进入告警规则页面，如下图所示。

规则名称	一级分类	二级分类	级别	全部	状态	全部	查询	清空		
<input type="checkbox"/>	规则名称	级别	一级分类	二级分类	告警方式	状态	创建时间	类型	创建人	操作
<input type="checkbox"/>	test	非常低	内容安全	敏感邮件		启用	2017-11-14 14:17:28	自定义	operator	  
<input type="checkbox"/>	系统事件	中	TSM	TopAnalyzer		启用	2017-11-08 15:18:19	系统内置	operator	  
<input type="checkbox"/>	JMS转发失败	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:12	系统内置	operator	  
<input type="checkbox"/>	主机认证失败	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:11	系统内置	operator	  
<input type="checkbox"/>	目标主机不可达	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:10	系统内置	operator	  
<input type="checkbox"/>	资产插线	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:09	系统内置	operator	  
<input type="checkbox"/>	存储上限告警	中	TSM	TopAnalyzer		启用	2014-12-17 00:00:08	系统内置	operator	  
<input type="checkbox"/>	存储已达上限	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:07	系统内置	operator	  
<input type="checkbox"/>	主动日志源异常	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:06	系统内置	operator	  
<input type="checkbox"/>	节点插线	高	TSM	TopAnalyzer		启用	2014-12-17 00:00:05	系统内置	operator	  


**步骤 2** 点击列表上方的“”新建，进入新建页面。告警规则需要配置两方面的内容：

1) 基本信息：填写告警名称，选择类别、级别，设置超时时间，是否启用。



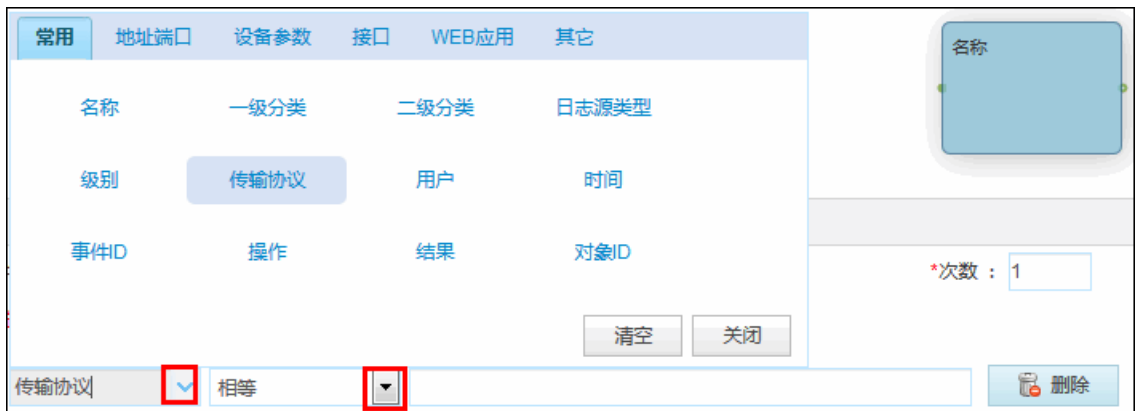
◇描述信息支持使用变量，如：`%LOGS[0].SRC_ADDRESS%` 表示第一条日志的源地址。

2) 告警规则：设置规则名称、响应时间、次数以及具体的规则信息等。点击告警规则

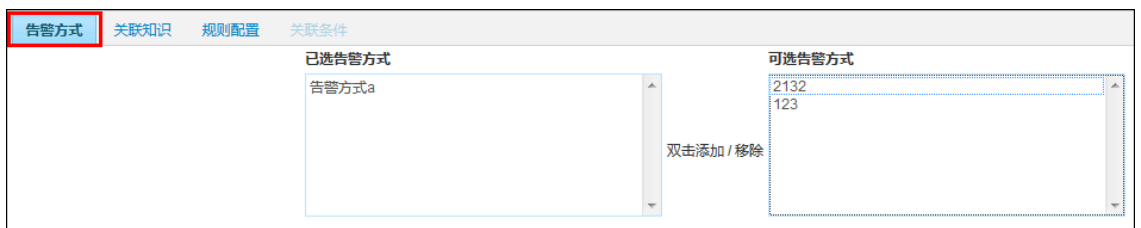
右侧的“”，进入告警规则设置页面。如下图所示。



规则配置：通过点击“添加条件”，在出现的条件设置处进行设定。第一个下拉列表选择条件参数，包括常用、地址端口、设备参数、接口、WEB应用和其它；第二个下拉列表根据条件参数列出不同的逻辑关系，包括相等、不相等、非空、包含、不包含、正则等；第三个文本框填写条件值，如下图所示。



告警方式：双击选择告警的方式，目前系统内包括声音、声光、命令等，如下图所示。



关联知识：点击“关联知识”页签下的“关联知识库”，用户可通过勾选知识库名称前的复选框设置告警规则关联一个或多个知识库，如下图所示。

知识库列表				
名称: <input type="text"/>				
<input type="checkbox"/> 名称	时间	分类1	分类2	
<input checked="" type="checkbox"/> 知识库测试01	2017-11-13 15:23:57	信息破坏	信息假冒	
<b>解决方案:</b> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">           解决方法         </div>				
<input checked="" type="checkbox"/> 知识库测试02	2017-11-13 15:31:22	信息破坏	信息假冒	
<input type="checkbox"/> 知识库测试03	2017-11-13 16:09:17	信息破坏	信息窃取	

10 | 第 1 共 1 页 | 显示 1 到 3, 共 3 记录

►关联条件：创建两个告警规则后方可设置关联条件。点击两个告警规则框之间的箭头，可设置告警规则关联条件。如下图所示。

**告警规则配置**

基本信息 → 关联告警方式

---

**基本信息**

\*名称:  \*一级分类: 请选择 \*二级分类: 请选择  
 \*级别: 非常低 \*超时时间: 5 秒 是否启用:

描述:

---

**告警规则**

→

---

告警方式 关联知识 规则配置 **关联条件**

应用协议:  相等  从 资产掉线 到 主动日志源异常

主动日志源异常: 资产掉线(应用协议-相等)

\*双击删除

从第一个下拉框中选择关联字段，从第二个下拉框中选择关联属性，然后点击右侧的【添加】即可。

**步骤 3** 设置完成后点击【保存】即可。

点击某个规则所在行的“”编辑，进入编辑页面进行修改，完成后点击“保存”即

**步骤 4** 可。



✧只允许对自定义的告警规则执行编辑修改操作。

---

通过点击规则名称前的复选框选择一个或多个规则后,点击


“”

启用或

“”


禁用完成告警的启停操作。

**步骤 5**

点击某个规则所在行的“”复制,进入告警规则设置页面,新的告警规则可以完成复

**步骤 6**

用原有的设置,用户只需要为规则重新命名即可。


点击某个规则所在行的“”打开告警响应方式列表,用户通过名称前的复选框选择一

**步骤 7**

个或多个告警方式即可,此处与新建告警规则中的 [告警方式](#) (See 5.7.3.2) 功能相同。




<input type="checkbox"/> 名称	响应方式	创建者	状态
<input type="checkbox"/> 邮件告警	邮件响应	operator	禁用
<input type="checkbox"/> 声音响应	声音响应	operator	禁用
<input type="checkbox"/> 声音告警	声音响应	zjc	禁用
<input type="checkbox"/> 声光告警	声光响应	operator	禁用
<input type="checkbox"/> 声光	声音响应	zjc	启用
<input type="checkbox"/> 命令告警	执行本地命令	operator	启用

点击某个规则所在行的“”，打开知识库列表，如下图所示。用户通过名称前的复选框选择一个或多个知识库，此处与新建告警规则中的 [关联知识](#) (See 5.7.3.2) 功能相同。

**步骤 8**

<input type="checkbox"/> 名称	时间	一级分类	二级分类
<input checked="" type="checkbox"/> 知识库测试01	2017-11-13 15:23:57	信息破坏	信息假冒
<input checked="" type="checkbox"/> 知识库测试02	2017-11-13 15:31:22	信息破坏	信息假冒
<input checked="" type="checkbox"/> 知识库测试03	2017-11-13 16:09:17	信息破坏	信息窃取

10 | 第 1 共 1 页 | 显示 1 到 3, 共 3 记录

通过点击规则名称前的复选框选择一个或多个规则后，点击“”删除，在出现的对话框进行确认即可。

**步骤 9**

通过设置规则名称、一级分类、二级分类、级别、状态，点击【查询】可以查看相应的告警规则。

**步骤 10**

### 5.7.3.3 告警过滤规则

告警过滤规则主要用于配置告警规则过滤条件。匹配上告警过滤规则的事件则不进行告警。

**步骤 1** 选择 **配置 > 系统配置 > 告警过滤规则**，进入告警过滤规则配置页面，如下图所示。

告警过滤规则配置									
告警名称:	设备地址:	源地址:	目的地址:	状态: 全部	查询	清空			
<input type="checkbox"/> 告警名称	设备地址	源地址	目的地址	告警描述	时间间隔(分钟)	速度	状态	操作	
<input type="checkbox"/> 日志重复		192.168.78.31	192.168.1.65		60	0	启用		
<input type="checkbox"/> 主机认证失败		172.19.8.14	123.36.32.23		60	0	启用		
<input type="checkbox"/> 主动日志源异常		152.36.25.36	127.0.0.1		60	0	启用		
<input type="checkbox"/> 主动日志源异常		192.168.75.50	127.0.0.1		60	0	启用		

**步骤 2** 点击列表上方的“”新建，进入新建页面。如下图所示。

#### 告警过滤规则配置

1、如果告警名称、设备地址、源地址、目的地址、描述中任何一个字段为空表示此字段匹配所有告警。  
2、速度表示在时间间隔内，最多触发该告警的次数，如果速度设置为0表示屏蔽所有符合此规则的告警。

告警名称

设备地址

源地址

目的地址

告警描述

\*时间(分钟)

\*速度

是否启用  启用

各参数的具体说明如下：

参数	说明
告警名称	设置告警过滤规则名称。
设备地址	设置产生告警事件的设备 IP。
源地址	设置告警事件的源地址。
目的地址	设置告警事件的目的地址
告警描述	设置对此告警事件的描述信息。
时间（分钟）	设置屏蔽告警规则的时间间隔，单位为分钟。
速度	设置屏蔽告警规则的速度，即在时间间隔内最多触发该告警的次数。如果速度指定为 0 表示屏蔽所有符合此规则的告警。
是否启用	勾选后启用该告警过滤规则。

**步骤 3** 设置完成后点击【保存】即可。

点击某个规则所在行的“”编辑，进入编辑页面进行修改，完成后点击【保存】即可。

**步骤 4** 可。

通过点击规则名称前的复选框选择一个或多个规则后，点击“”启用或“”禁用

**步骤 5** 完成告警的启停操作。

**步骤 6** 通过设置告警名称、源地址、目的地址、状态，可以查询告警规则。

## 5.7.3.4 告警方式管理

通过将告警事件与响应方式关联配置，当系统检测到不安全的告警事件时就会以相应的形式及时通知管理员进行处理，从而保障系统的安全运行。系统可以通过声音、邮件、Snmp Trap、执行本地命令等方式发出响应。

**步骤 1** 选择 **配置 > 系统配置 > 告警方式管理**，进入告警管理页面，如下图所示。

告警方式管理							
名称:		响应方式:		 查询	 清空		
 新建		 启用		 禁用		 删除	
<input type="checkbox"/>	名称	响应方式	节点	创建者	描述	状态	操作
<input type="checkbox"/>	test	执行本地命令	127.0.0.1	operator	fds	禁用	
<input type="checkbox"/>	邮件告警	声音响应	127.0.0.1	operator	ddd	启用	
<input type="checkbox"/>	rere	声音响应	127.0.0.1	operator		启用	

步骤 2 点击“新建”按钮添加告警方式，如下图所示。设置告警方式的名称、描述信息后，在“响应方式”下拉框中选择告警的响应方式。



告警方式管理

\*名称

\*绑定节点 127.0.0.1

\*响应方式

描述



◇描述信息支持使用变量，如：`%LOGS[0].SRC_ADDRESS%` 表示第一条日志的源地址。

➤ 选择声音响应

声音响应是指当系统中的日志或事件匹配了告警规则时，系统会发出已定义的声音，进行告警。



\*响应方式 声音响应

描述

\*等级 等级一

\*循环次数

\*间隔时间(秒)

各参数的具体说明如下：

参数	说明
等级	设置响应声音，包括 5 个等级，每个等级都有不同的声音。
循环次数	设置声音响应的循环次数。
间隔时间	设置每次声音响应的循环间隔，单位：秒。

➤ 选择 Snmp Trap

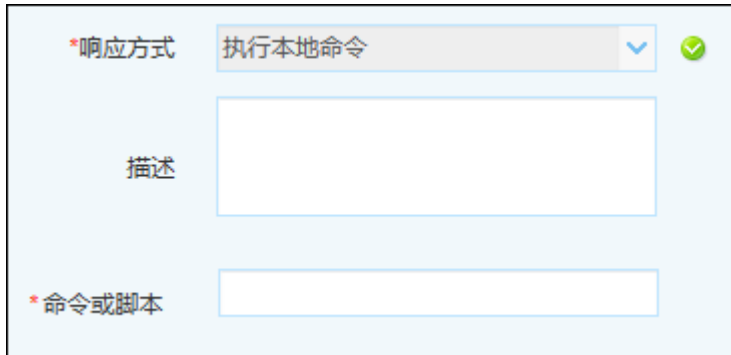
Snmp Trap 是指当系统中的日志或事件匹配了告警规则时，系统会发送 SNMP Trap 消息进行告警。

各参数的具体说明如下：

参数	说明
SNMP 协议版本	选择 SNMP 协议版本，可选项包括：SNMP V1 和 SNMP V2C。
SNMP 通信字	设置 SNMP 通信字，一般为 public，管理员可以根据需要自行设定。
传输协议	设置传输协议，目前只支持 UDP。
服务器 IP 地址	设置接收 SNMP Trap 消息的 SNMP 服务器 IP 地址。
端口	设置服务器端口。

➤ 选择执行本地命令

执行本地命令是指当系统中的日志或事件匹配了告警规则时，系统会自动执行管理员设定的可执行程序，进行响应。在“命令或脚本”栏内输入本地已存在的可执行程序的路径和名称。



The screenshot shows a configuration window for a response action. At the top, the label '\*响应方式' (Response Method) is followed by a dropdown menu set to '执行本地命令' (Execute Local Command) and a green checkmark icon. Below this is a large empty text box labeled '描述' (Description). At the bottom, there is a label '\*命令或脚本' (Command or Script) followed by an empty text input field.

➤ 选择声光响应

声光响应是指当系统中的日志或事件匹配了告警规则时，系统会自动发出声音并弹出通知框进行报警。



The screenshot shows a configuration window for a 'Sound and Light Response'. At the top, the label '\*响应方式' (Response Method) is followed by a dropdown menu set to '声光响应' (Sound and Light Response) and a green checkmark icon. Below this is a large empty text box labeled '描述' (Description). Further down, the label '\*等级' (Level) is followed by a dropdown menu set to '等级一' (Level 1). At the bottom, there is a label '通知内容' (Notification Content) followed by an empty text input field.

各参数的具体说明如下：

参数	说明
等级	选择报警等级，有五个等级，不同的等级有不同的报警声音。
通知内容	设置通知内容。

➤ 选择邮件响应

邮件响应是指当系统中的日志或事件匹配了告警规则时，邮件服务器会自动发邮件给收信人，及时响应。

The screenshot shows a configuration panel with the following fields:

- \*响应方式**: 邮件响应 (with a dropdown arrow and a green checkmark icon)
- 描述**: A large empty text area.
- \*标题**: An empty text input field.
- \*通知内容**: A large empty text area.
- 邮件**: An empty text input field with a '+' button to its right.
- \*邮件地址**: An empty text input field with a '-' button to its right.

各参数的具体说明如下：

参数	说明
标题	设置邮件标题
通知内容	设置邮件内容
邮件\邮件地址	设置将邮件响应信息发送到哪些地址，格式如 123@topsec.com.cn

➤ 选择短信响应

短信响应是指当系统中的日志或事件匹配了告警规则时，系统在内网范围内会自动发送消息给指定的电话号码进行报警。

（短信响应需要短信猫的支持，具体信息请联系天融信公司技术人员。）

The image shows a configuration window for SMS response. The fields are as follows:

- \*响应方式**: 短信响应 (SMS Response)
- 描述**: (Empty text box)
- \*标题**: (Empty text box)
- \*内容**: (Empty text box)
- 电话**: (Empty text box with a "+" button)
- \*电话号码列表**: (Empty list box with "-" button)
- \*连接时使用(N)**: (Empty dropdown menu)
- \*每秒位数(B)**: 9600 (Dropdown menu)

各参数的具体说明如下：

参数	说明
标题	设置短信标题
内容	设置短信内容
电话	设置接收短信的手机号码后，点击右侧的“+”按钮，便可将设定的电话号码加入到下方的“电话号码列表”中。
电话号码列表	显示接收告警短信的手机号码列表。在列表中，选中某个电话号码，并点击右侧的“-”按钮，可将该号码从列表中移除。
连接时使用	选择与短信猫连接的接口。
每秒位数	设置短信猫接口的比特率。可选项：9600、57600、115200。

➤ 选择一信通响应

一信通响应是指当系统中的日志或事件匹配了告警规则时，系统连接企业一信通平台发送消息给指定的电话号码进行报警。



各参数的具体说明如下：

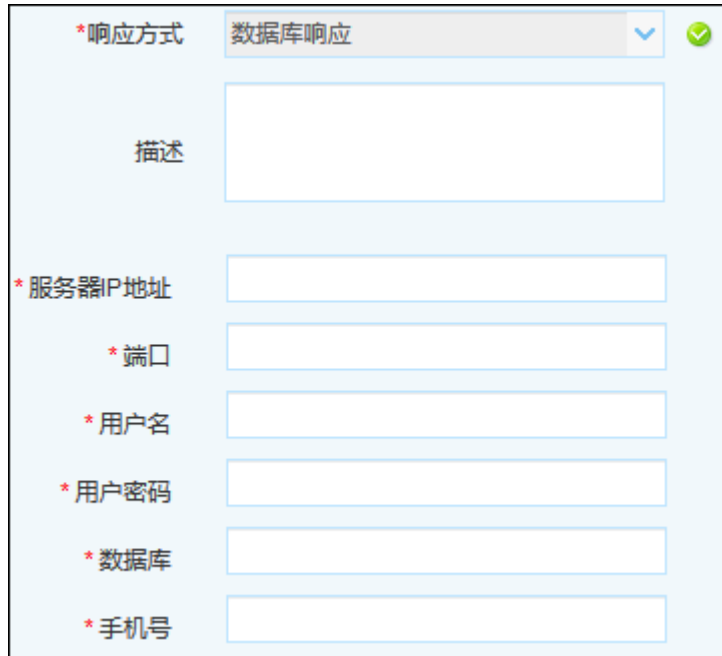
参数	说明
企业编号	输入一个正确的准入企业编号。
用户名称	输入收信方的用户名称。
用户密码	输入收信方的登录准入用户密码。
短信内容	输入短信内容。
电话	设置接收短信的手机号码后，点击右侧的“+”按钮，便可将设定的电话号码加入到下方的“电话号码列表”中。
电话号码列表	显示接收告警短信的手机号码列表。在列表中，选中某个电话号码，并点击右侧的“-”按钮，可将该号码从列表中移除。



◇告警方式中执行本地命令、声光、邮件、短信限速机制 1 分钟 10 次。

►选择数据库响应

数据库响应是指当系统中的日志或事件匹配了告警规则时，系统通过数据库服务器发送消息给指定的电话号码进行报警。



各参数的具体说明如下：


参数	说明
服务器 IP 地址	输入数据库所在服务器的 IP 地址。
端口	输入数据库所使用的端口号。
用户名	输入登录数据库的用户名。
用户密码	输入登录数据库的用户密码。
数据库	输入数据库的名称。
手机号	设置接收告警短信的手机号码。

各参数设置完成后，点击【保存】按钮即可完成报警方式的添加，点击【测试】可在绑定节点的服务器上测试告警方式是否设置成功。

**步骤 3**

点击告警方式管理页面对应的启用、禁用、删除按钮可以实现相应操作。点击告警方式

**步骤 4**

对应的编辑图标“”，可对告警方式进行修改。

## 5.7.3.5 邮件服务器

在邮件告警以及计划报表中，邮件服务器负责将告警信息或报表信息发给收信人。邮件服务器的配置步骤如下：

**步骤 1** 以操作管理员身份登录系统后，选择 **配置 > 系统配置 > 邮件服务器**，进入“邮件服务器配置”页面，如下图所示。

**描述** 邮件告警以及计划报表中，发送邮件所使用的邮件服务器信息。

*邮件服务器地址	192.168.79.3
*邮件服务器端口	26
*邮件发送人	admin@126.com
*用户名	admin
*口令	*****
SSL连接	<input type="checkbox"/> 是

参数说明见下表：

参数	说明
邮件服务器 ip	设置邮件服务器 IP 地址。
邮件服务器端口	设置邮件服务器端口。
邮件发送人	设置发信方的 Email 地址。
用户名	发信方登录邮件系统的用户名。
口令	发信方登录邮件系统的口令。
SSL 连接	允许邮件服务器 SSL 连接，则可以向外网邮件服务器的发送邮件。

**步骤 2** 参数设置完成后，点击【应用】按钮即可。

## 5.7.3.6 采集器端口

采集器端口主要用来设置各种日志和流量采集器的端口，其设置步骤如下：

**步骤 1** 选择 **配置 > 系统配置 > 采集器端口**，进入“采集器端口配置”页面，如下图所示。

**采集器端口配置**

描述 Syslog SNMP NetFlow的端口配置。

**Syslog端口配置**

+  
514  
515 -

**SNMP端口配置**

+  
162  
163 -

**Netflow端口配置**

+  
9991  
9999 -

应用

在各个采集器端口的文本框中输入端口号后，点击“+”按钮即可将端口加入到该采集

**步骤 2** 器端口中。在已设置端口框中选择一个端口，点击“-”按钮即可将该端口删除。

**步骤 3** 参数设置完成后，点击【应用】按钮即可。



◇采集器端口如果绑定失败则会产生审计日志，反之正常收集日志信息。

## 5.7.3.7 节点管理

此处的节点包含了系统本身、直属代理节点、下级节点以及告警节点。只有预置操作管理员可以对代理进行删除和启用自保护的操作，自定义操作管理员只能查看。节点管理可以对代理和服务端进行升级操作。



◇只有预置操作管理员可以对代理/告警节点执行删除和启用自保护的操作，自定义操作管理员只能查看代理/告警信息。

选择 **配置 > 系统配置 > 节点管理**，进入节点管理页面，如下图所示。

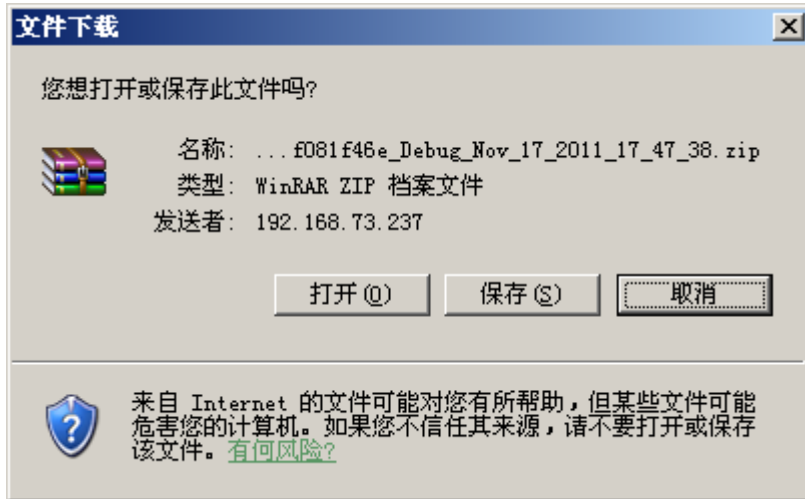
### 步骤 1

名称	状态	全部	IP地址	查询	清空	服务器升级	代理升级
状态	名称	IP地址	类型	版本	运行时间	操作	
1	●	auditor	127.0.0.1	服务器	3.3.3.09_Win	3天3小时10分钟31秒	
2	●	action	127.0.0.1	告警节点	3.3.3.09_Win	3天3小时9分钟56秒	
3	●	172.17.30.129	172.17.30.129	下级	3.3.3.09_Win	3天3小时9分钟40秒	
4	●	agent	192.168.25.102	代理	3.3.3.09_Win	0秒	
5	●	agent	192.168.25.102	代理	3.3.3.09_Win	0秒	
6	●	action	192.168.25.102	告警节点	3.3.3.09_Win	0秒	

在此页面，可以查看代理的状态、名称、IP地址、类型、版本等信息。其中状态字段显示绿色表示节点连接正常，显示灰色表示节点不在线。“操作”一栏中的“”表示未启动自保护机制，“”表示启动自保护机制，即启动后用户无法手动终止代理相关进程。如果无法启动自保护机制，请确认在安装本系统时 TopDesk\_X64 程序是否安装成功。

### 步骤 2 下载诊断信息

诊断信息包括系统最近运行期间保留下来的日志信息，这些信息有助于帮助管理员诊断系统故障。点击代理相应操作栏中的下载诊断信息图标“”，弹出文件保存对话框，如下图所示。选择路径后，点击“保存”按钮完成下载。



对于不再使用的代理，可以点击代理对应的删除图标“”进行删除。但是无法删除当

### 步骤 3 前服务器。

- 服务器升级

天融信日志收集与分析系统支持在线升级，服务器升级是指对本级服务器进行升级，具体的升级方法为：

**步骤 1** 选择 **配置 > 系统配置 > 节点管理**，进入如下图的页面。

节点管理							
名称	状态	全部	IP地址	查询	清空	服务器升级	代理升级
状态	名称	IP地址	类型	版本	运行时间	操作	
1	● auditor	127.0.0.1	服务器	3.3.3.09_Win	2天3小时21分钟22秒		
2	● action	127.0.0.1	告警节点	3.3.3.09_Win	2天3小时20分钟47秒		
3	● 172.17.30.129	172.17.30.129	下级	3.3.3.09_Win	2天3小时20分钟31秒		
4	● agent	192.168.25.102	代理	3.3.3.09_Win	0秒		
5	● agent	192.168.25.102	代理	3.3.3.09_Win	16分57秒		
6	● action	192.168.25.102	告警节点	3.3.3.09_Win	0秒		

**步骤 2** 点击“服务器升级”，进入如下页面。



**步骤 3** 点击【浏览】按钮，选择升级包。

**步骤 4** 点击【应用】按钮进行升级。升级完成后，系统会自动重启。

● 代理升级

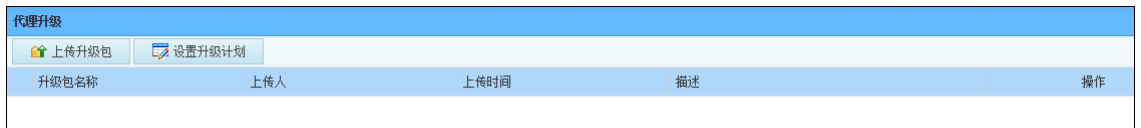
代理升级是指对本级节点的直接代理进行升级。将代理节点的升级包上传系统后，管理员可以制定升级计划，进而可实现代理节点的自动升级。实现代理升级的具体方法为：

**步骤 1** 选择 **配置 > 系统配置 > 节点管理**，进入如下图的页面。



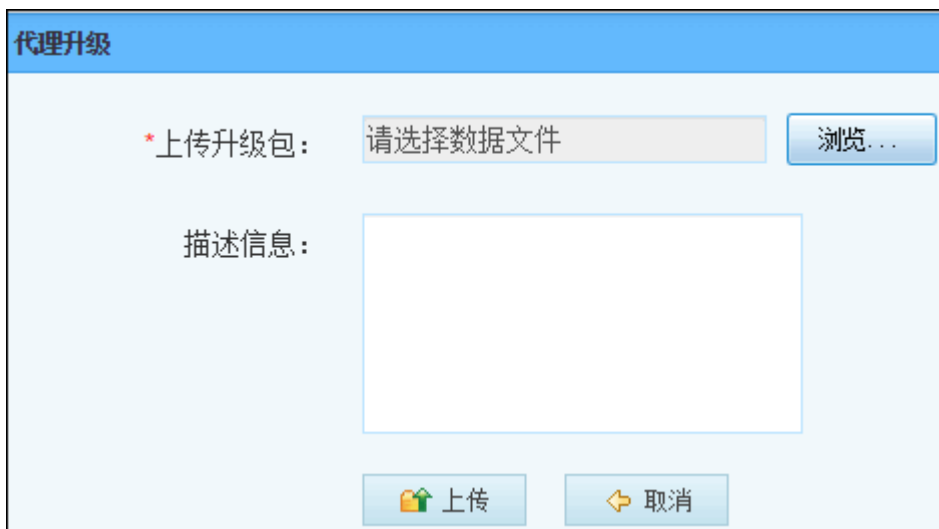
节点管理							
名称	状态	全部	IP地址	查询	清空	服务器升级	代理升级
状态	名称	IP地址	类型	版本	运行时间	操作	
1	●	auditor	127.0.0.1	服务器	3.3.3.09_Win	2天3小时21分钟22秒	📄
2	●	action	127.0.0.1	告警节点	3.3.3.09_Win	2天3小时20分钟47秒	📄
3	●	172.17.30.129	172.17.30.129	下级	3.3.3.09_Win	2天3小时20分钟31秒	📄
4	●	agent	192.168.25.102	代理	3.3.3.09_Win	0秒	📄 🔄 ✓
5	●	agent	192.168.25.102	代理	3.3.3.09_Win	16分57秒	📄 🔄 ✓
6	●	action	192.168.25.102	告警节点	3.3.3.09_Win	0秒	📄 🔄 ✓

**步骤 2** 点击“代理升级”，进入如下界面。



代理升级				
上传升级包		设置升级计划		
升级包名称	上传者	上传时间	描述	操作

**步骤 3** 点击“上传升级包”，进入如下图的页面。



**代理升级**

\*上传升级包:

描述信息:

点击【浏览】按钮选择升级包文件，并填写描述信息后，点击【上传】按钮，便可将升级包上传至系统中。

**步骤 4** 在升级包列表页面，点击“设置升级计划”，弹出设置升级时间页面，如下图所示。



如果只需执行一次升级，则选择“特定时间执行一次”，并在下方设置升级时间；如果需要定期执行升级，则选择“周期性”，并在下方设置升级的间隔周期。

设置完成后，点击【应用】按钮，完成升级时间设置。到达设定时候后，系统会自动对代理进行升级操作。

**步骤 5**

## 5.7.3.8 系统备份

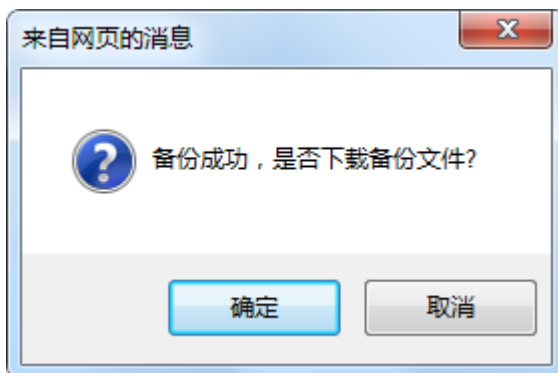
系统备份是将当前系统的配置信息备份，以便系统重装以后直接导入系统备份文件，而不用再次配置。下面详细介绍系统备份的具体操作步骤。

**步骤 1** 选择 **配置 > 系统配置 > 系统备份**，进入系统备份页面，如下图所示。



点击【备份】按钮开始备份，备份成功后，弹出询问是否下载备份文件的对话框，如下图所示。

**步骤 2**



**步骤 3** 点击【确定】按钮，便可将备份文件保存至本地。




## 5.7.3.9 资源管理

资源管理主要用于标识业务网段，便于管理员区分 IP 地址/IP 网段对应的业务网络。当管理员设置 IP 地址/IP 地址网段资源后，在日志查询界面中，如果日志的“源地址”、“目的地址”字段内容为资源对应的地址，将鼠标指针移动到日志的“源地址”/“目的地址”字段上，可显示地址对应的资源名称，关于日志的查看请参见 [日志查询](#) (See 5.2.3)。

**步骤 1** 选择 **配置 > 系统配置 > 资源管理**，进入资源管理页面，如下图所示。



名称	IP地址	操作
1	2.2.2.2	
hxj	192.168.25.107	
lkk	127.0.0.1	

**步骤 2** 点击“”，进入新增 IP 地址界面，如下图所示。



IP地址名称管理 | IP地址网段管理

\*名称

\*IP地址

保存 返回

用户输入名称、IP 地址，然后点击【保存】即可。

**步骤 3** 激活“IP 地址段管理”页签，如下图所示。



IP地址名称管理 | IP地址网段管理

\*名称

\*起始IP地址

\*结束IP地址

保存 返回

用户输入名称、起始 IP 地址、结束 IP 地址，然后点击【保存】即可。

在“名称”和“IP 地址”文本框中输入需要查找的内容，点击【查询】，查询结果显示在下方列表中。

**步骤 4**

**步骤 5** 选中一行后点击“”完成删除操作。

## 5.7.3.10 设备支持列表


通过选择 **配置 > 系统配置 > 设备支持列表**，便可查看 TA-L 系统所支持的所有设备信息，如下图所示。

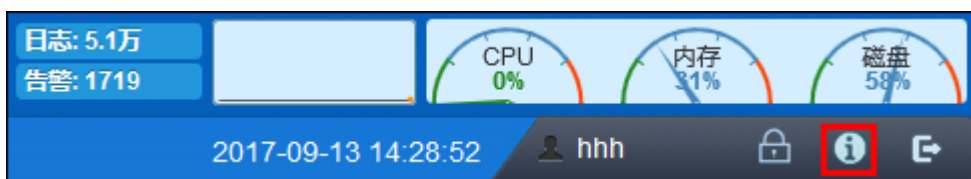
类型	厂商	版本
AJMR	天融信	JMR
安管平台	网神	安管平台
AntiDos	天融信	TopDDOS , TopADS
	H3C	DptechDDOS
	Huawei	AntiDDOS
	绿盟	Defender
	思科	Guard
AntiVirus	KingSoft	KingsoftVGM
	网神	防毒墙
AVG	天融信	TopFilter
	Intel	McAfee Webshield
	趋势	防毒墙
	赛门铁克	端点防护管理系统V11

界面中列出了 TA-L 系统所支持的所有设备型号、厂商和版本信息。用户可以将其导出为 Excel、Word 格式的文件。

## 5.8 关于

在“关于”页面可以查看产品版本信息和产品许可信息，也可下载收集代理和告警节点的安装包，具体操作为：

**步骤 1** 在系统页面，点击页面右上方的关于图标“”，如下图所示。



步骤 2 进入“产品信息”页面，如下图所示。



页面展示了产品的名称、版本、许可类型、过期时间、许可日志源数、已使用日志源数等信息。

点击“Agent 下载”图标，可以下载收集代理安装包；点击“告警节点下载”图标，可以下载告警节点安装包。

步骤 3

步骤 4 升级系统许可证

点击【浏览】按钮选择 license 文件，并点击【上传】按钮，可以升级系统许可文件。



◇只有将设备的机器码提交给天融信技术支持人员，方可获得设备相应的 License 文件。硬 key 升级除外。

步骤 5 获取设备机器码

1) 进入获取机器码界面。进入获取机器码界面有三种方式，具体如下：

- 当设备 Licence 已经过期时，在浏览器中输入以下地址：<http://ip/sim/sysman/licensegen.jsp>，其中“ip”指设备具体的 IP 地址。例如：<http://192.168.73.241/sim/sysman/licensegen.jsp>。
- 当设备 Licence 未过期时，在浏览器中输入以下地址：<http://ip/page/sysconfig/licensegen.jsp>，其中“ip”指设备具体的 IP 地址。例如：<http://192.168.73.241/page/sysconfig/licensegen.jsp>。
- 点击系统“关于”页面中的【获取机器码】按钮。

**获取服务器机器码**

**描述** 请输入公司名称来获取对应的服务器机器码。

**公司名称**

**服务器机器码**

复制到粘贴板

返回登录页面

2) 输入公司名称后，点击“服务器机器码”文本框，服务器机器码会显示，如下图所示。

**获取服务器机器码**

**描述** 请输入公司名称来获取对应的服务器机器码。

**公司名称**

**服务器机器码**

01010c4591cc6b2abbee50e9f0bdb02fbd8ce0f786938b2e4f  
 00015e76d19400,01010c4591cc6b2abbee50e9f0bdb02fbd  
 8ce0f786938b2e4f00015e76d19400,01010c4591cc6b2abb  
 ee50e9f0bdb02fbd8ce0f786938b2e4f00015e76d19400,010

复制到粘贴板

返回登录页面

3) 点击【复制到粘贴板】按钮将此机器码复制，发送给天融信支持人员，便可得到相应的 Licence 文件。

#### 步骤 6 管理授权地址

点击【授权地址管理】按钮，如下图所示。




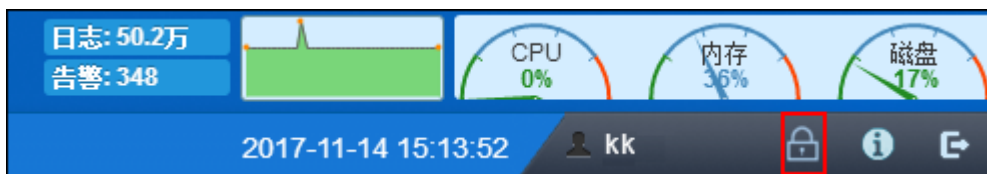
管理员输入起始 IP、结束 IP 和有效期后，点击【生成授权地址】按钮，生成授权地址，备份该授权地址，指定 IP 地址范围内的用户输入该 URL 可进行登录，登录后具有和当前管理员相同的权限。

**需要说明的是**，审计管理员没有“生成授权地址”功能。

## 5.9 锁定

锁定功能可锁定当前操作界面，执行锁定操作后，页面被锁定，待用户输入解锁密码再次进入系统时，界面显示内容仍旧为锁定前内容。主要用于解决系统空闲超时后，管理员无法进入系统超时前的操作界面。

**步骤 1** 当用户停留在某个页面上时，点击界面右上角的“”，如下图所示。



**步骤 2** 进入锁定页面，如下图所示。



**步骤 3** 输入账户密码，待用户再次进入系统时，界面显示内容为锁定前内容。

## 6. 审计管理员

审计管理员（预置账户为：auditor/talent123）拥有主页、日志管理、报表管理和查看产品信息的权限，但是只能管理和查看系统自身产生的日志及相关报表。

相关内容包括：

- [主页](#) (See 6.1)：主要显示最近时间段内日志的统计和告警信息。
- [日志](#) (See 6.2)：主要介绍日志的查询和备份管理。
- [报表](#) (See 6.3)：主要介绍基本报表和计划报表的查看和相关配置。

### 6.1 主页

审计管理员登录系统后即进入系统主页，如下图所示。



在此，审计管理员可以查看日志源、系统拓扑、日志信息、告警信息等，具体的说明请参见**操作管理员**的[主页](#)(See 5.1)，**需要注意的是**，**审计管理员**主页菜单下没有任何子菜单项，系统预置**操作管理员**的主页菜单下包含“总览”和“本级”两个子菜单项。

## 6.2 日志

审计管理员由于权限的原因只能查看“日志摘要”、“日志查询”和“备份管理”三个子菜单的内容，支持查看所有节点操作管理员和系统管理员的审计日志，查看步骤与操作管理员的日志查看方式类似，具体请参见**操作管理员**的[日志](#)(See 5.2)的相关内容。

## 6.3 报表

报表管理模块主要包含基本报表和计划报表两种，主要介绍审计日志统计报表的查看和定制计划报表，并进行报表管理和定时报表任务管理等操作，支持导出各种形式的报表，满足管理员不同的需求。

相关内容包括：

- [基本报表](#) (See 6.3.1)
- [计划报表](#) (See 6.3.2)

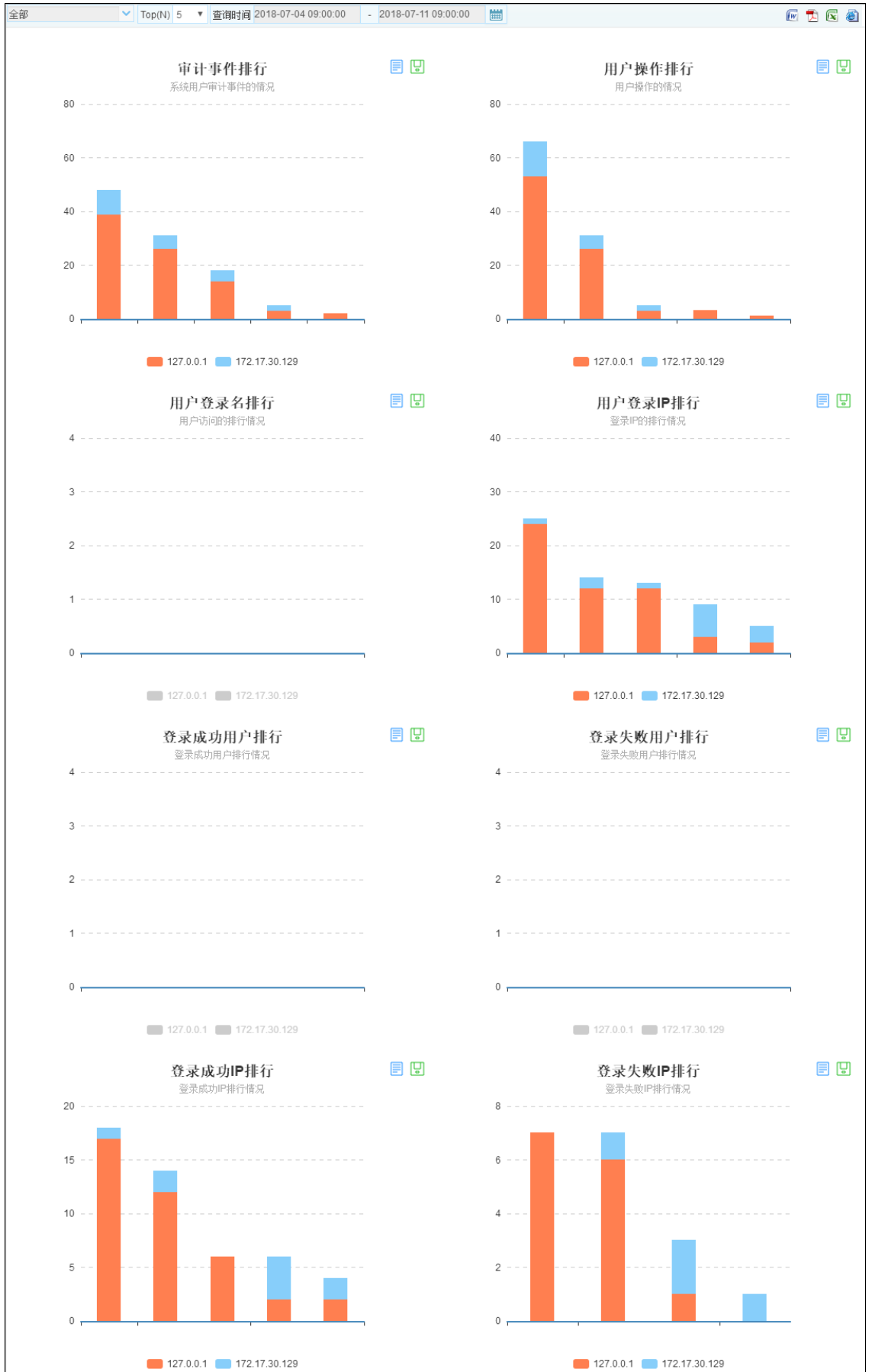
---

## 6.3.1 基本报表

在基本报表中，审计管理员可查看全部节点（本级节点和下级节点）的审计日志统计报表。

选择 **报表** > **基本报表**，在左侧导航栏中选择“审计报表”，展开审计报表，选择“**步骤 1** 审计日志统计”，进入“报表数据展示”界面，如下图所示。

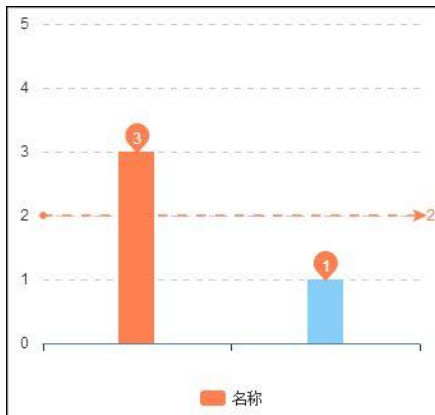




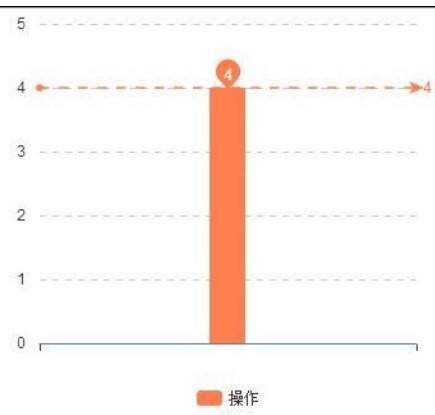
---

默认显示全部节点最近一小时的审计日志信息。用户可自定义查询条件，包括节点选择、Top(N)和查询时间。

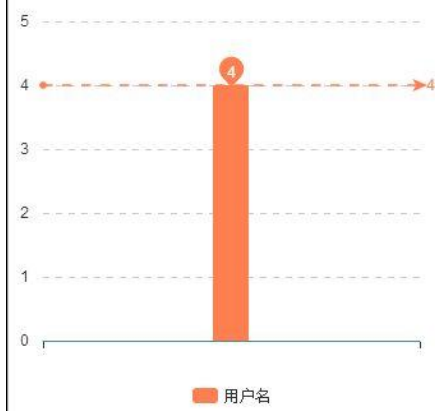
查看单个节点的报表信息时，统计图中会显示平均值和最高、最低数据值。界面效果如下图所示：



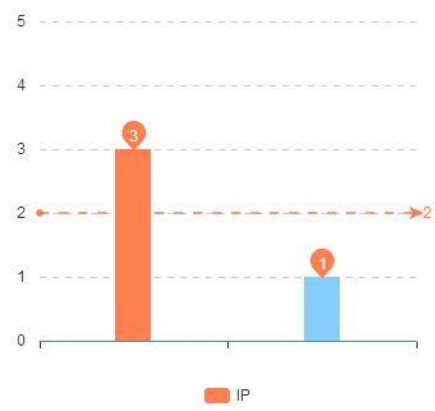
用户登录名排行  
用户访问的排行情况



用户登录IP排行  
登录IP的排行情况



登录成功用户排行  
登录成功用户排行情况



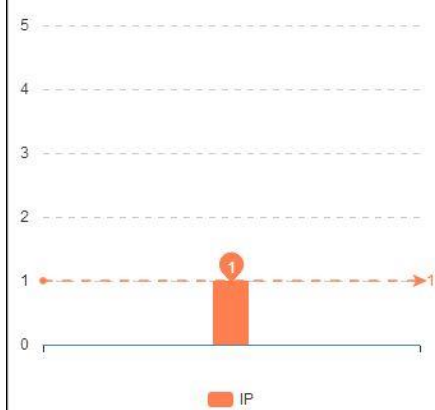
登录失败用户排行  
登录失败用户排行情况



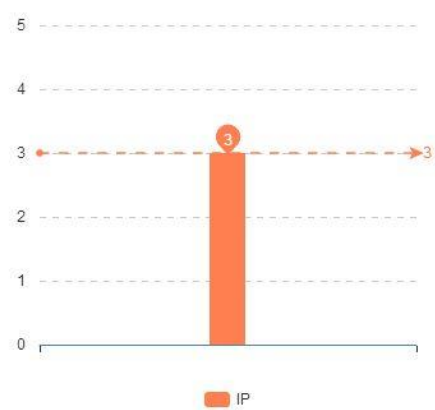
登录成功IP排行  
登录成功IP排行情况




登录失败IP排行  
登录失败IP排行情况




IP



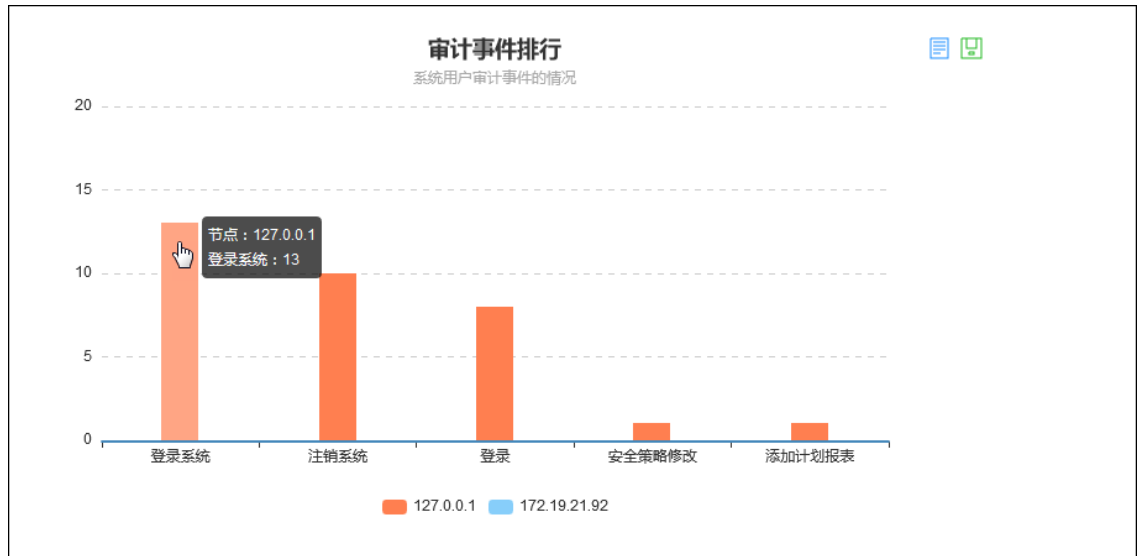
IP





审计报表分为“审计事件排行”、“用户操作排行”、“用户登录名排行”、“用户登录 IP 排行”、“登录成功用户排行”、“登录失败用户排行”、“登录成功 IP 排行”和“登录失败 IP 排行”。点击统计图右上角的“”图标可将柱状统计图转换为数据

**步骤 2** 视图：点击“”图标可将柱状统计图保存为图片。

单击柱状图相应位置可跳转至审计日志查询界面，并将该柱状统计图的横坐标作为审计日志的查询条件进行快速查询，无需在 **日志 > 日志查询** 界面单独设置查询条件，操作简便快捷。鼠标悬停在此可查看详细信息，如下图所示。

**步骤 3**









点击页面右上角的“   ”中的相应图标，可分别导出 doc、pdf、excel、html 格式的报表。

**步骤 4**

## 6.3.2 计划报表

系统不仅能够实时查询报表、设置个性化报表、保存报表为多格式的文件，还可以定期定时发送报表到指定的邮件账户，满足了用户有规律接收报表、定期了解设备情况的需求。系统可以设定在每年、每月、每周或每天的某个时间，将含有记录特定时间特定节点审计日志的报表的电子邮件发送到指定的收件人。设置计划报表的具体步骤如下：

**步骤 1** 选择 **报表 > 计划报表**，进入计划报表界面，如下图所示。

名称	类型	用户	导出格式	收件人邮箱	报表类型	下次执行时间	最近编辑时间	状态	操作	下载
报表2	基础信息报	auditor	excel	hu_xiaojuan@topsec.com.c	日报表	22日 8时30分	2017-09-21 11:15:1	启用		
报表1	基础信息报	auditor	pdf	hu_xiaojuan@topsec.com.c	日报表	13时30分	2017-09-21 11:13:3	启用		
qq	基础信息报	auditor	pdf	hu_xiaojuan@topsec.cn	日报表	22日 4时4分	2017-09-21 11:10:0	启用		

**步骤 2** 点击【新建】按钮，弹出添加计划报表的界面，然后指定计划报表类型为“基本报表”，

如下图所示。

管理员也可在左侧的导航树中单击“每天执行”、“每周执行”、“每月执行”和“每年执行”，在弹出的界面中新建计划报表。


在新建计划报表时，各项参数的具体说明如下表所示。

参数	说明
名称	设置计划报表的名称。
执行时间	设置生成统计报表的时间。可设置每天、每周、每月和每年执行。
计划报表类型	可选项：基本报表。
设备报表主题	选择具体的报表主题。
时间类型	设置报表的时间类型，包括：天报表、周报表、月报表、年报表。
数据 Top (N)	设置对 Top (N) 的数据进行统计，可选项包括：Top5、Top10、Top15、Top20 和 Top25。
导出文件格式	选择导出文件格式，包括：word 文件、pdf 文件、excel 文件和 html 文件。
邮件地址	输入报表收信人的邮箱地址，例如： <a href="mailto:abc@topsec.com.cn">abc@topsec.com.cn</a> 。

参数	说明
已选邮件地址	点击“+”，添加邮箱地址，可以添加多个邮箱地址；点击“—”，移除已添加的邮箱地址。 <b>需要说明的是：</b> 邮件发送功能需要同时配置邮件服务器，请参见 <a href="#">配置 &gt; 系统配置 &gt; 邮件服务器</a> 。

参数设置完成后，点击页面右下角的【保存】按钮即可完成新建计划报表的操作。新建的计划报表可在计划报表列表中显示，管理员可对其进行编辑、删除、启用和禁用操作。

### 步骤 3

对于执行成功的任务，管理员点击相应行的“”可下载.zip 格式的报表文件到本地；

**步骤 4** 点击【执行结果】按钮查询，可查看计划报表任务的执行情况。

管理员也可在左侧的导航树中单击“每天执行”、“每周执行”、“每月执行”和“每年执行”分别查看相应类型的计划报表。

点击【清空】按钮可清空执行结果，点击【返

**步骤 5 回】**按钮返回到新建计划报表的界面。



◇ 新建的计划报表默认是启用状态，用户可选中指定的计划报表，点击【禁用】按钮禁用指定的计划报表任务。

## 7. 账户管理员

账户管理员可对系统账户进行统一维护和管理，包括新建（只有预置的账户管理员 admin 才有创建用户的权限）、编辑、删除和查询账户，还可设定整个系统的安全策略，即密码复杂度和登录超时自动退出等。

相关内容包括：

- [主页](#) (See 7.1)：主要显示最近时间段内日志的统计和告警信息。
- [用户](#) (See 7.2)：主要介绍用户管理和安全管理。

### 7.1 主页

账户管理员登录系统后即进入系统主页，如下图所示。



账户管理员可查看系统的日志和告警信息，具体说明请参见操作管理员的 [主页](#) (See 5.1) ，**需要注意的是**，主页菜单下没有任何子菜单项，操作管理员的主页菜单下包含“总览”和“本级”两个子菜单项。

## 7.2 用户




账户管理员可对系统用户进行统一维护和管理，包括新建、编辑、删除和查询用户，还可设定整个系统的安全策略，即密码复杂度和登录超时自动退出等。

相关内容包括：

- [用户管理](#) (See 7.2.1) ：介绍如何创建用户，并对用户进行管理和维护。
- [安全管理](#) (See 7.2.2) ：介绍如何对用户登录系统的安全性进行管理。

### 7.2.1 用户管理


天融信日志收集与分析系统包含帐户管理员、操作管理员和审计管理员三种管理角色，不同的角色对系统拥有不同的管理权限：




- 帐户管理员：权限包括查看主页、进行用户管理、安全管理和查看产品信息（点击页面右上角的“”图标查看）。
- 操作管理员：权限包括主页、日志（日志摘要、实时日志、日志查询、备份管理和查询统计）、报表、日志源管理、知识库、配置、告警管理和查看产品信息（点击页面右上角的“”图标查看）。
- 审计管理员：权限包括查看主页、日志（日志摘要、日志查询和备份管理）、报表和查看产品信息（点击页面右上角的“”图标查看）。

每种角色帐户的设置类似，现以设置操作管理员为例说明具体的设置过程。

以帐户管理员身份登录系统后可以对系统内的用户进行管理，设置操作管理员的操作如下：

**步骤 1** 以账户管理员身份登录系统，选择 **用户 > 用户管理**，进入用户管理页面，如下图所示。



名称	所属角色	状态	有效期	创建者	最后修改时间	操作
Wsj	操作管理员	启用	2018-07-31 14:03:00	admin	2018-07-10 15:03:47	 
hxj	操作管理员	启用	2018-07-31 13:44:12	admin	2018-07-10 13:33:12	 
qk_oper	操作管理员	启用	2018-07-07 14:53:42	admin	2018-06-28 14:44:39	 
Zx	操作管理员	启用	2018-07-07 14:00:27	admin	2018-06-28 13:51:38	 
auditor	审计管理员	启用	2104-01-25 05:20:00	admin	2018-07-09 10:28:46	 
operator	操作管理员	启用	2104-01-25 05:20:00	admin	2018-06-27 14:03:52	 

**步骤 2** 点击【新建】按钮，弹出添加新账户窗口，如下图所示。



### 新建用户

用户名:

IP地址范围:  至

有效期:

状态:  启用

密码:

确认密码:

所属角色: 操作管理员 ▼

全部

选择权限:

▲

▼

选择

删除

描述:

保存

取消

在新建用户时，各项参数的具体说明如下表所示。

参数	说明
用户名	设置该管理员的登录名称。
IP 地址范围	设置可使用该账号登录系统的 IP 地址范围，即范围之外的 IP 地址不可以使用该账号登录系统。
有效期	设置可使用该账号登录系统的有效日期，即在有效期之外该帐号是不可用的。
状态	帐户状态默认为禁用，勾选“启用”后，方可使用该帐户。

参数	说明
密码	设置该帐户的登录密码。关于密码长度和复杂度的设置，请参见 <a href="#">安全管理</a> (See 7.2.2)。
确认密码	再次输入该帐户的密码。
所属角色	管理员所属的角色类型，包括：帐户管理员、操作管理员和审计管理员。
选择权限	点击【选择】按钮，设置该管理员可以查看哪些设备的信息。 说明： 仅在添加“操作管理员”时，需要设置此参数，只有添加权限后，新创建的“操作管理员”才可对相关日志源的日志进行操作。
描述	选填项，设置管理员的相关描述信息。

### 步骤 3 修改/清空账户管理员登录 IP 范围

点击【修改登录 IP 范围】按钮，如下图所示。

**修改登录IP范围**

1、起始IP、结束IP如果为空表示没有限制  
 2、最小起始IP为0.0.0.0,最大结束IP为255.255.255.255  
 3、如果由于修改错误无法在允许的登录IP范围内登录，请到服务器上使  
 用127.0.0.1登录账号再修改登录IP范围

起始IP (包含) : 1.1.1.1  
 结束IP (包含) : 223.254.254.254

保存 取消

用户可在起始 IP 和结束 IP 处修改登录 IP（结束 IP 必须大于等于起始 IP），从而改变 admin 账户登录 IP 范围。同时可点击【清空登录 IP】按钮，取消 admin 账户登录 IP 范围限制。



◇ 如果由于修改错误无法再允许的登录 IP 范围内登录，请到服务器上使用 127.0.0.1 登录账号再修改登录 IP 范围。

用户信息设置完成后，点击【保存】按钮，完成管理步骤4 修改或删除该帐户。



operator 和 auditor 是系统预置角色，不能进行删除操作。

系统初始的管理员角色（operator、admin 和 auditor）相对于新建的相应的用户角色拥有更高的权限，可查看的菜单项会有所不同，具体以登录界面为准。

## 7.2.2 安全管理

安全管理主要包括密码安全和登录安全管理（如果 TA-L 所在的服务器有上级节点，则会有如下图所示的【请求策略】按钮，用于向上级节点请求同步安全策略；如果 TA-L 所在的服务器有下级节点，则会有【下发策略】按钮，用于向下级节点下发安全策略）。现以有上级节点的服务器为例进行介绍。具体设置步骤如下：

**步骤 1** 以帐户管理员身份登录系统后，选择 **用户 > 安全管理**，如下图所示。

### 密码安全

最少字符数:

最少包含大写字母数:

最少包含小写字母数:

最少包含多少数字:

密码更新周期:  (天)

### 登录安全

登录失败多少次后锁住IP:

多长时间不操作自动退出登录:  (分钟)

### 系统配置

安全检测:  启用

在设置安全管理的相关参数时，各项参数的具体说明如下表所示。

参数		说明
密码安全	最少字符数	设置用户登录密码的最小长度，范围：8-32。
	最少包含大写 字母数	设置用户密码中最少需要包含多少个大写字母。
	最少包含小写 字母数	设置用户密码中最少需要包含多少个小写字母。
	最少包含多少 数字	设置用户密码中最少需要包含多少个数字。
	密码更新周期	设置用户密码的更新周期，即多长时间更新一次密码。 密码更新周期到期后，系统会强制用户修改密码。 此策略对所有账户生效。
登录安全	登录失败多少 次后锁住 IP	设置某个账号最多尝试登录的次数，超过设定次数后该 IP 地址将被系统锁定，系统默认锁定时间为 3 分钟。
	多长时间不操 作自动退出登 录	设置账号登录后的空闲时间。 若该账号在此设定时间内未对系统进行任何操作，将自 动退出系统。
系统配 置	安全检测	勾选该选项，表示系统会对输入框中输入的内容进行安 全性检查。

参数设置完成后点击【应用】按钮保存配置；如需向上级节点同步安全策略，点击【请求策略】按钮即可进行安全策略的同步。