

# 科来网络回溯分析系统

## 产品安装配置手册

# 科来网络回溯分析系统

## 产品安装配置手册

本手册主要为您提供科来网络回溯分析系统的操作与配置，请仔细阅读并妥善保存，以备需要时使用。

感谢您对科来产品的支持。

© 2011 科来软件 保留所有权利

科来软件

电话：010-82601814

传真：010-82601614

网址：<http://www.colasoft.com.cn>

## 目录

<b>目录</b> .....	<b>2</b>
<b>产品部署</b> .....	<b>3</b>
1. 分析服务器部署.....	3
2. 分析控制台.....	3
3. 产品部署示意图.....	4
<b>分析服务器配置</b> .....	<b>4</b>
1. 硬件面板.....	4
2. 接口配置.....	5
3. 服务器参数配置.....	5
3.1. 接口设置.....	6
3.2. 管理接口设置.....	7
3.3. 网络链路设置.....	8
3.4. 用户管理设置.....	11
3.5. 其它设置.....	12
<b>分析控制台安装</b> .....	<b>13</b>
1. 软件安装.....	13
2. 添加分析服务器.....	16
<b>服务与技术支持</b> .....	<b>17</b>
1. 服务项目与说明.....	17
2. 技术服务中心.....	18

## 产品部署

科来网络回溯分析系统采用软硬件一体化设计,由分析服务器与分析控制台组成。分析服务器作为整个产品的核心,用于网络通讯数据的实时采集和分析,它是网络回溯分析系统的部署重点,如果部署有误,将会采集不到需要的数据,影响产品的正常使用。我们建议在需要被监控和分析的网络链路上部署分析服务器,以便采集和分析关键链路的通讯数据。

### 1. 分析服务器部署

分析服务器通常提供 4 个或以上网络采集接口,根据不同的网络环境或用户需求,可采用分路器或端口镜像进行网络通讯数据的采集。如果采用端口镜像的方式进行数据采集,首先需要在交换机做端口镜像,将需要监控的网络链路流量镜像到分析服务器的数据采集口。

#### 端口镜像配置:

按照以下步骤进行端口镜像配置操作:(以 Cisco Catalyst 4000 系列交换机端口镜像为例)

假如交换机的上联口为 f5/48,即该端口连接路由器,为了捕获整个网络的数据通讯,因此,我们需要将该端口作为被镜像口(即被监控口),将该端口的数据复制到我们指定的监控口,此处以 f5/1 为例,即 f5/1 作为镜像端口(监控口),再将分析服务器的任意一个采集口(参加图 2 硬件面板图)接在 f5/1 端口即可。基于以上需求,端口镜像配置如下:

#### 配置被镜像端口:

```
Switch(config)# monitor session 1 source interface fastethernet 5/48
```

#### 配置镜像端口:

```
Switch(config)# monitor session 1 destination interface fastethernet 5/1
```

配置完成,可以查看配置:

```
Switch# show monitor session 1
```

**注:**不同厂家的交换机,端口镜像配置有所不同,具体操作配置可咨询厂家技术支持。

我们的官方网站提供了常见交换机的端口镜像配置方法,请访问:

[http://www.colasoft.com.cn/support/port\\_mirroring.php](http://www.colasoft.com.cn/support/port_mirroring.php)

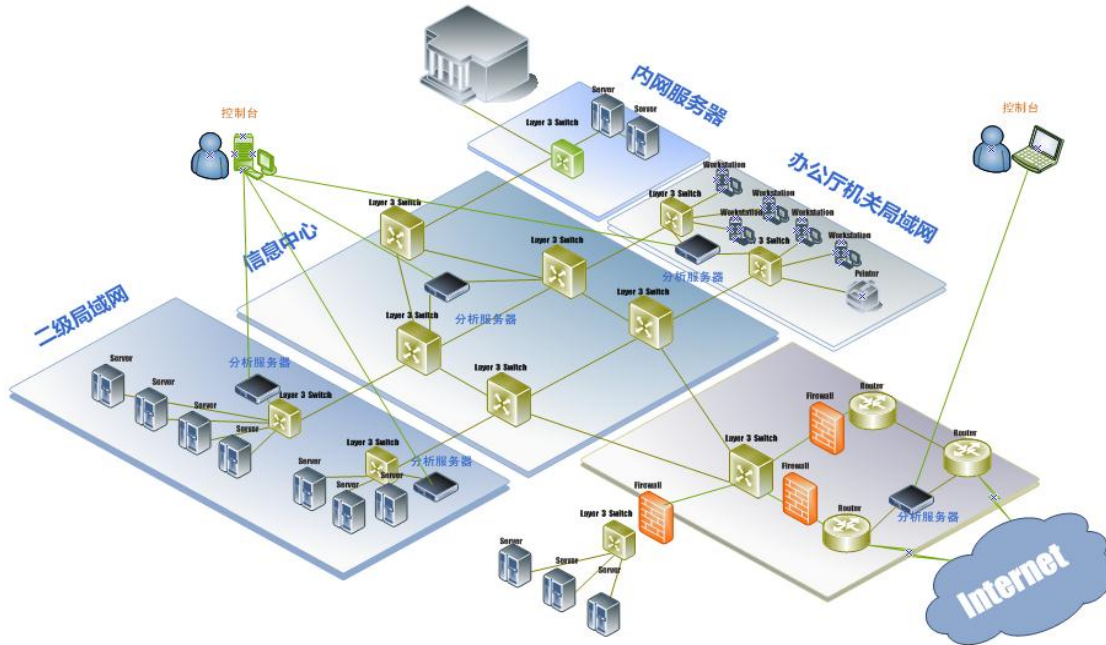
**提示:**借助分路器的部署请以具体的分路器类型为准,具体接线配置请参见分路器说明。

### 2. 分析控制台

分析控制台用于连接分析服务器进行数据查看和分析,采用便携式软件安装包,只需安装在能够正常接入 Internet 的计算机上即可,如工作站或笔记本电脑。

## 3. 产品部署示意图

产品的部署示意图如下（图1）：

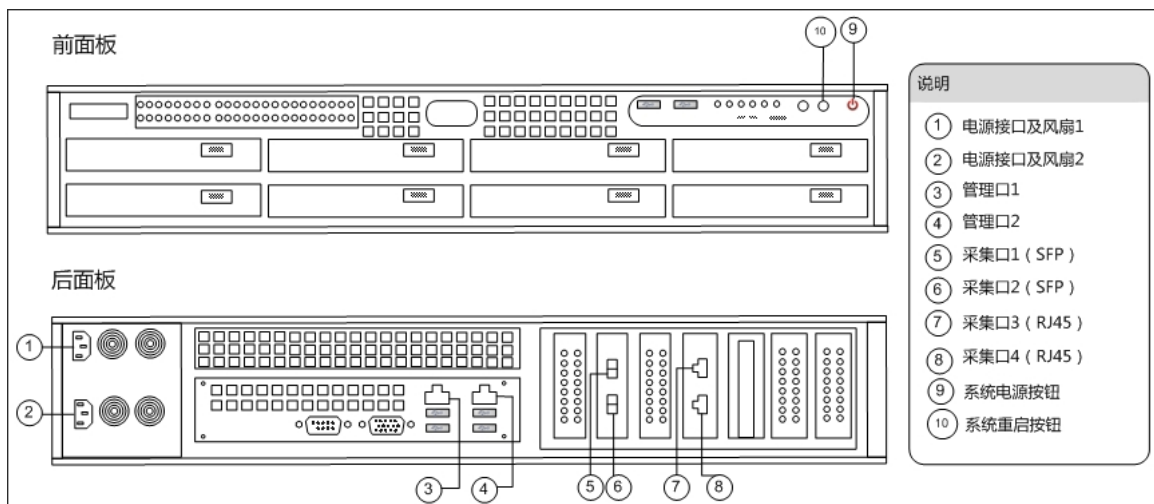


（图1 产品部署示意图）

## 分析服务器配置

### 1. 硬件面板

分析服务器硬件面板示意图如图2所示：（RAS3000系列）



（图2 服务器面板图）

分析服务器提供了 2 个管理口（图中所示的③和④接口）和 4 个采集口（图中所示的⑤、⑥、⑦和⑧接口）。管理口用于服务器基本参数配置，采集口用于网络通讯数据采集。

**注意：不同系列、不同型号的分析服务器，其硬件面板及网络接口会略有不同，详细的硬件面板接线图请参见服务器背板上的贴图。**

## 2. 接口配置

分析服务器在初次使用时，需要进行以下初始配置：

### ☐ 管理口：

由于管理口用于服务器参数配置，因此，需要通过连接管理口进入服务器 Web 配置界面。用任意一台 PC（首先将该 PC 的 IP 地址设置为 192.168.5.160/161）连接图 2 中的③管理口即可（管理口④暂时保留）。

### ☐ 采集口：

网络接口⑤、⑥、⑦和⑧口为系统的数据采集口 1, 2, 3, 4，根据具体的部署方式，将交换机镜像监控口或分路器接入其中任意一个采集口即可。

## 3. 服务器参数配置

按照接口配置完成服务器接线后，打开浏览器，输入 <http://192.168.5.160>，登录服务器进行参数配置：



系统默认提供一个管理员帐号，输入默认用户名及密码，登录系统：

用户名：csadmin

密码：colasoft

分析服务器包括以下基本参数配置：

- 系统信息
- 接口设置
- 管理接口设置
- 网络链路设置
- 用户管理设置

### 3.1. 系统信息

系统信息页面能够查看和了解分析服务器的运行状态。

科来网络回溯分析系统 - 服务器参数配置

用户: admin | 帮助 | 安全退出

**系统设置**

- 系统信息
- 网络链路
- 用户管理
- 分析中心
- 接口设置
- 管理接口
- 审计日志

#### 系统信息

产品信息	
产品名称:	科来网络回溯分析系统
产品版本:	3.0.0.423
产品许可:	成都科来软件有限公司
产品授权:	已激活
产品序列号:	04E330-120F05-25300-110816-101002
授权用户:	科来软件
产品型号:	

服务器信息	
总内存:	3.960 GB
可用内存:	1.077 GB
内存使用率:	72%
CPU 使用率:	46%
磁盘信息:	统计数据磁盘: 291GB/465GB; 数据包磁盘: 111GB/465GB
开始时间:	2011/08/04 10:09:39
运行时间:	04:47:59

刷新   **重置系统**   重启系统   重启服务器   关闭服务器

版权所有 © 2011 成都科来软件有限公司      处理时间: 0.021594 秒

该页面提供以下 4 个功能按钮：

- 重置系统：单击此按钮，将暂停正在进行的链路监控，并且将清除所有保存的历史数据，包括统计数据及数据包，需谨慎使用；

- ☒ 重启系统：重置系统后，需要手动重启系统，单击此按钮，将重新启动系统；
- ☒ 重启服务器：重新启动分析服务器；
- ☒ 关闭服务器：关闭服务器，分析服务器将停止运行；

**提示：**请慎重使用此 4 个功能按钮，为避免不必要的麻烦，在使用之前，请确定已经完全了解各按钮的功能。

## 3.2. 接口设置

接口设置页面显示了系统安装的所有网络适配器，需要将各网络适配器接口类型根据实际情况设置为采集接口或配置接口，接口设置完成后，才能进入后续的网络链路设置及服务器基本信息查看。



科来网络回溯分析系统 - 服务器参数配置

用户: admin | 帮助 | 安全退出

系统设置

- 系统信息
- 网络链路
- 用户管理
- 分析中心
- 接口设置**
- 管理接口
- 审计日志

### 接口设置

接口名称	接口状态	连接速度(Mbps)	接口类型
采集口1	未连接	1000	采集接口 ▼
采集口2	未连接	1000	采集接口 ▼
管理配置口2 (192.168.5.160)	已连接	1000	配置接口 ▼
管理配置口1	未连接	1000	采集接口 ▼

保存

版权所有 © 2011 成都科来软件有限公司

处理时间: 0.149257 秒

根据图 2 所示的硬件面板示意图看到，服务器提供了 2 个管理口和 4 个采集口，在服务器出厂前，我们已经修改好网络适配器接口名称，用户可根据接口名称修改其对应的接口类型。

**注意：**不同版本的采集接口和配置接口的数量限制均不同，请仔细查看各个版本的功能说明。

## 3.3. 管理接口设置

一般情况下，分析服务器均提供两个网络接口用于分析服务器的配置与管理。管理接口设置页面可对管理接口的 IP 地址、网关、DNS 服务器等参数进行修改，服务器出厂前，我们已经设置其中一个管理接口的 IP 参数信息（默认 IP 地址：192.168.5.160）。根据图 2 的硬件面板图所示，接口③为我们设置的默认管理接口，接口④为保留接口，以备后续使用。

科来网络回溯分析系统 - 服务器参数配置 用户: admin | 帮助 | 安全退出

---

**系统设置**

- 系统信息
- 网络链路
- 用户管理
- 分析中心
- 接口设置
- 管理接口**
- 审计日志

### 管理接口 - 管理配置口2

---

IP地址:	<input type="text" value="192.168.5.160"/>
IP掩码:	<input type="text" value="255.255.255.0"/>
网关地址:	<input type="text" value="192.168.5.1"/>
DNS服务器:	<input type="text" value="61.139.2.69"/> (多个用逗号分隔)

---

---

版权所有 © 2011 成都科来软件有限公司 处理时间: 0.032004 秒

对于管理接口 IP 地址、网关 IP 地址以及 DNS 服务器，用户可以根据内网实际环境进行修改。

**注意：** 请谨慎修改通信 IP 地址，确保新的 IP 地址能够正常的进行 Internet 通讯。

### 3.4. 网络链路设置

科来网络回溯分析系统以网络链路为对象进行数据采集和分析，因此，在初次使用产品时，需要配置网络链路。打开服务器配置页面，单击“网络链路”，进入如下界面：

科来网络回溯分析系统 - 服务器参数配置 用户: admin | 帮助 | 安全退出

---

**系统设置**

- 系统信息
- 网络链路**
- 用户管理
- 分析中心
- 接口设置
- 管理接口
- 审计日志

### 网络链路 - 配置网络链路

网络链路名称:

流量捕捉方式:

---

版权所有 © 2011 成都科来软件有限公司 处理时间: 0.000640 秒

在该页面中，首先设置网络链路名称，用于快速标识链路，流量捕捉方式包括：

- 标准分路器
- 汇聚型分路器
- 交换机单向流量镜像
- 交换机双向流量镜像

**提示：**

1. 标准分路器方式需确定出网流量接口和进网流量接口；
2. 汇聚型分路器方式需确定一个或多个接口作为流量接口；
3. 交换机单向流量方式需确定出网流量接口和进网流量接口；
4. 交换机双向流量方式需确定一个或多个接口作为流量接口。



根据服务器的部署方式选择对应的流量捕捉方式，单击“下一步”，配置网络采集接口：

网络接口信息中，系统自动扫描并显示出当前安装的采集适配器的名称、状态、带宽等相关属性，用户可选择一块或多块网络适配器进行数据包捕捉。

根据选择的流量捕捉方式，下一步配置页面会稍有不同。

例如：

1. 选择交换机双向流量或汇聚型分路器的捕捉方式时，需继续配置用户网络环境中的内网 IP 网段，以此区分 IP 类型、流量方向以及更准确的统计进/出网流量；
2. 选择标准型分路器或交换机单向流量捕捉方式时，则需继续指定进网流量接口或出网流量接口。

**注意：**选择双向流量的网络链路配置页面中，需要根据服务器的实际部署位置和内网子网划分进行 IP 网段的添加。如服务器部署在网络出口，需要捕获和分析整个网络的通讯，此时，需要将所有内网子网添加到 IP 网段配置中，从而能够更准确的统计收/发流量。同时，需要指定出网带宽及进网带宽，以准确统计进/出网利用率、进/出网流量等数据。

网络链路添加完成后，即可开始/停止网络链路流量捕获，单击统计按钮，可以查看捕获的流量数据，同时也可修改/删除链路。

科来网络回溯分析系统 - 服务器参数配置 用户: admin | 帮助 | 安全退出

- 系统设置
- 系统信息
- 网络链路**
- 用户管理
- 分析中心
- 接口设置
- 管理接口
- 审计日志

### 网络链路

编号	链路名称	链路类型	接口数量	状态	操作
1	网络出口	交换机双向流量镜像	1	运行中	<input type="button" value="修改"/> <input type="button" value="删除"/> <input type="button" value="停止"/> <input type="button" value="统计"/>
2	HTTP服务器	交换机双向流量镜像	1	运行中	<input type="button" value="修改"/> <input type="button" value="删除"/> <input type="button" value="停止"/> <input type="button" value="统计"/>

版权所有 © 2011 成都科来软件有限公司 处理时间: 0.000627 秒

### 3.5. 用户管理设置

用户管理设置页面中，管理员可以添加系统新用户，添加用户类型包括管理员及普通用户两种角色。

科来网络回溯分析系统 - 服务器参数配置 用户: admin | 帮助 | 安全退出

---

**系统设置**

- 系统信息
- 网络链路
- 用户管理**
- 分析中心
- 接口设置
- 管理接口
- 审计日志

### 用户管理 - 添加新用户

---

用户名:

登录密码:

确认密码:

备注:

类型:

帐号停用

---

版权所有 © 2011 成都科来软件有限公司 处理时间: 0.001903 秒

分析控制台连接分析服务器时，需要输入正确的用户名与密码，才能连接服务器进行数据查看和分析，此处添加的新用户用于分析控制台连接服务器时的登录认证。

#### 注意：

**普通用户：**当控制台使用普通用户登录服务器后，只能查看系统数据，不能配置修改系统参数。

**管理员：**管理员拥有普通用户的所有权限，并且能对服务器配置进行修改。

请根据需要增加适合的系统用户帐号。

### 3.6. 其它设置

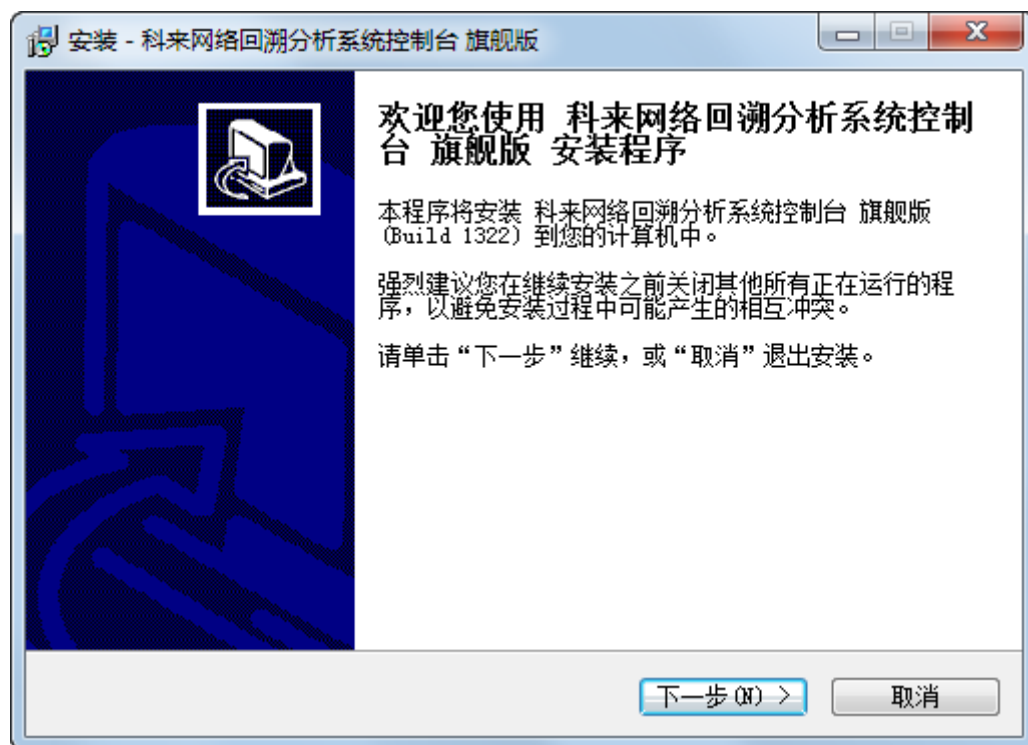
除基本设置外，服务器参数配置还包括分布式分析中心设置、系统信息以及审计日志查看。

- 分析中心：分析中心为系统的可选组件，如果没有购买该组件，则可以忽略该项配置；
- 系统信息：可以查看详细的系统产品信息及硬件运行信息，如 CPU 状态、内存使用率等；
- 审计日志：可以查看系统运行及用户的关键操作日志；

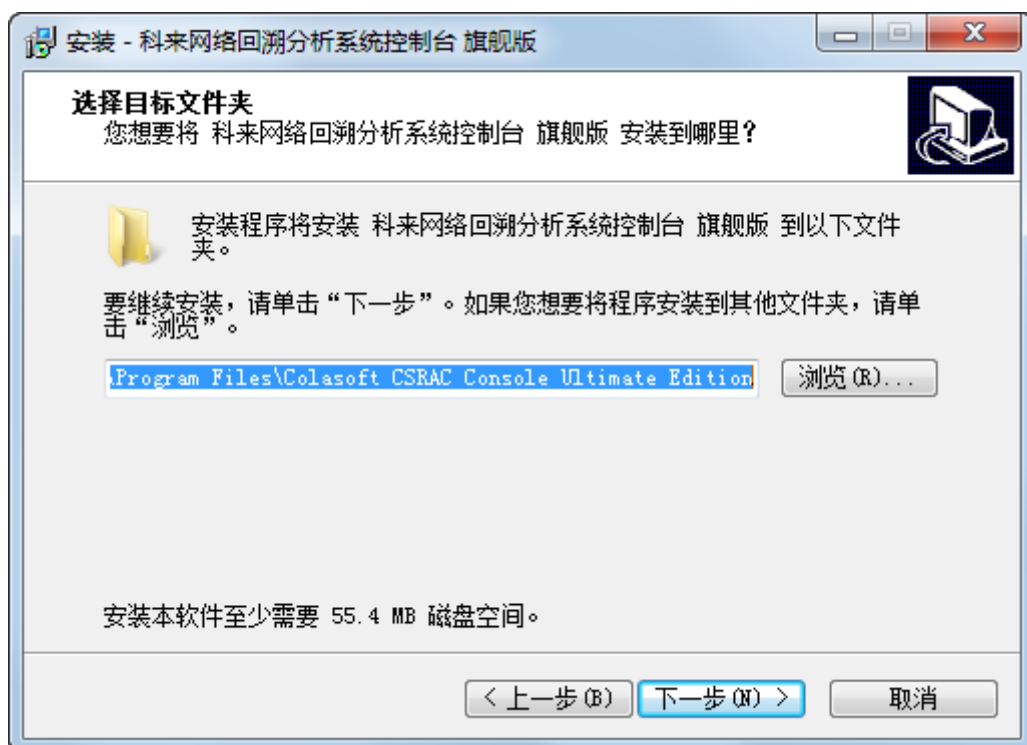
## 分析控制台安装

### 1. 软件安装

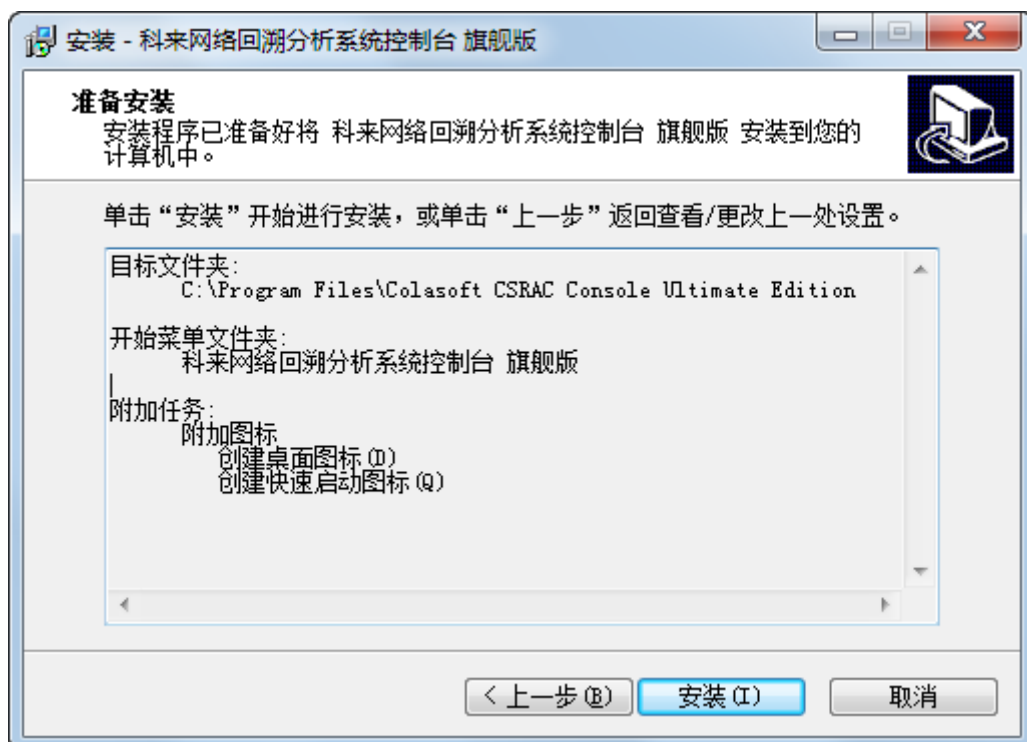
双击光盘中分析控制台 Setup 安装文件，弹出以下安装向导：



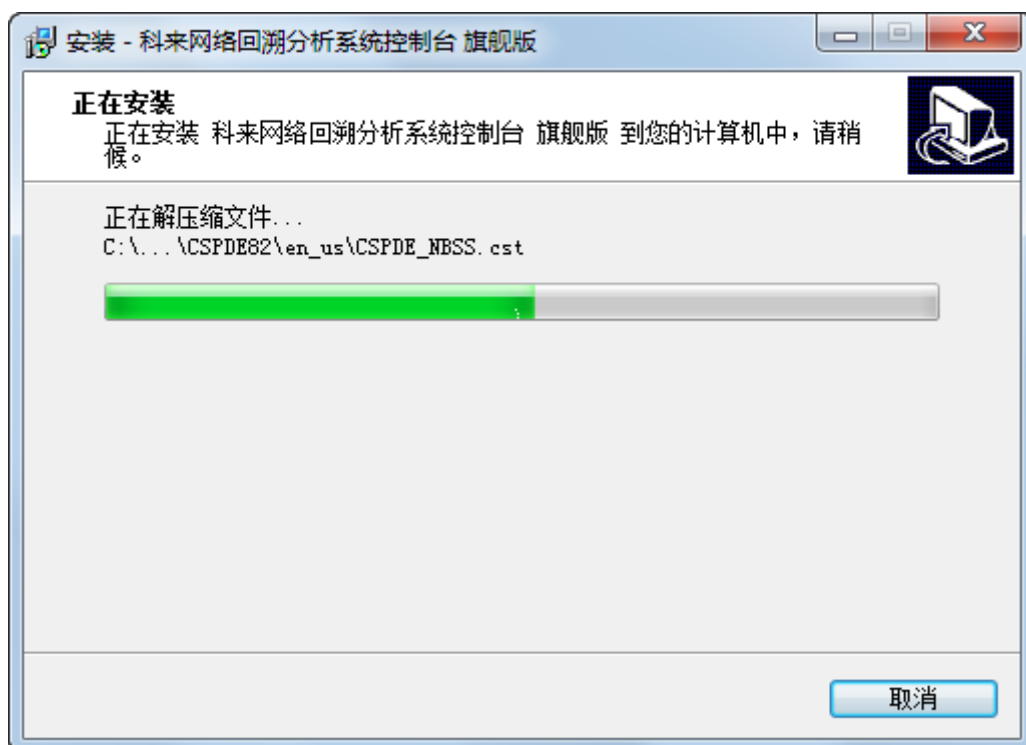
单击“下一步”，选择程序安装路径：



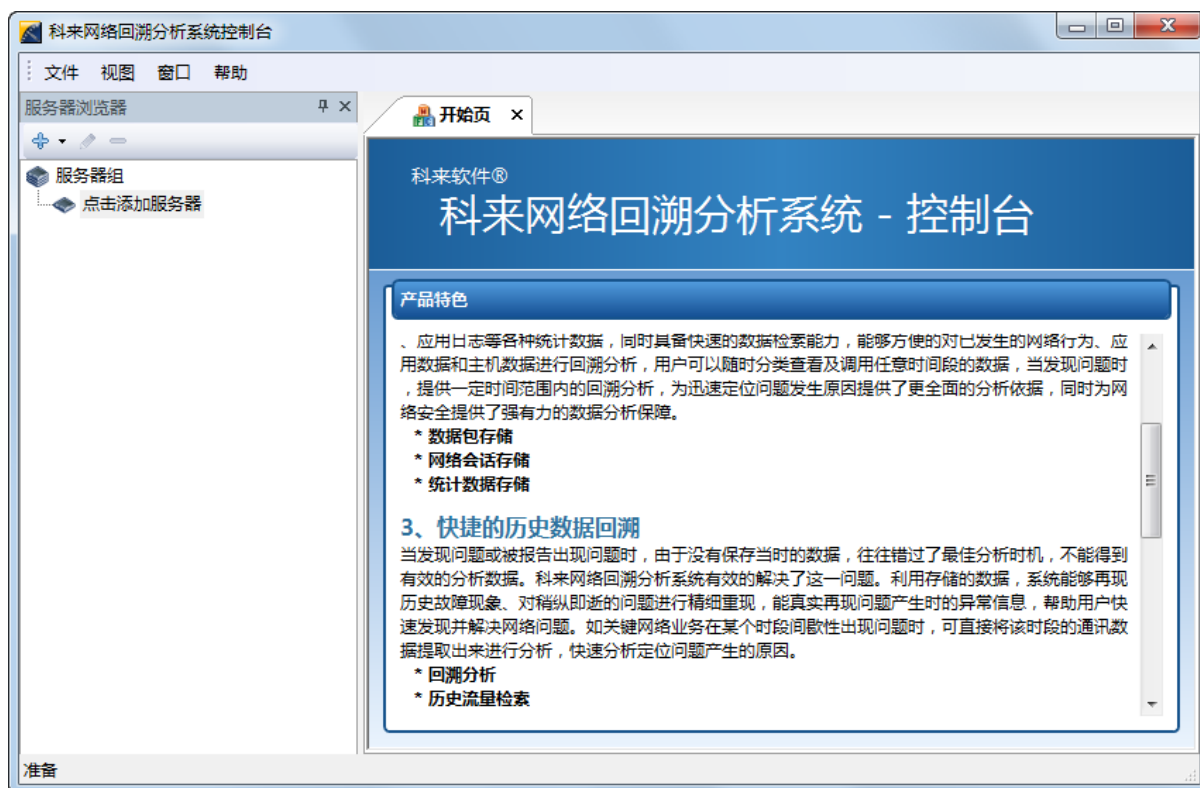
根据界面提示，可以选择按照默认路径也可修改为其他路径，直接单击“下一步”：



设置完毕，单击“安装”，开始安装分析控制台程序：



安装完成，即可使用分析控制台。



## 2. 添加分析服务器

初次使用分析控制台，需要添加分析服务器，在控制台主界面导航栏的服务器选项卡中，单击“添加服务器按钮”或单击右键菜单，添加服务器页面如下图：



- ☑ 地址：输入分析服务器 IP 地址，请参见服务器参数配置的[基本信息](#)章节；
- ☑ 端口：默认 3000；
- ☑ 登录名及密码：由分析服务器指定，请参见服务器参数配置的[用户管理](#)章节；
- ☑ 服务器显示名：输入服务器显示别名，方便标识。

**注意：端口号不可自行修改！**

添加完成，控制台显示如下：



展开服务器，可看到其下的网络链路，此时，可开始/停止网络链路监控。

- 1) 点击“开始监控”按钮，即启动链路监控分析（如果在服务器参数配置设置中已启动网络链路监控，此处则可以停止监控）。
- 2) 点击“打开”按钮，打开监控视图进行网络回溯分析。

## 服务与技术支持

### 1. 服务项目与说明

科来产品实行全国范围联保。无论您在中华人民共和国境内（不包括港、澳、台地区）何处使用，出现保修范围内的硬件故障时，可拨打科来服务热线 400-6869-069，服务人员将为您安排就近的科来技术支持服务机构提供保修服务。

#### ☐ 电话咨询服务

科来提供 3 年 5×8 小时电话咨询。如果您在电脑硬件方面遇到任何问题，你随时可以拨打服务热线电话 400-6869-069 寻求帮助，我们的工程师将为您提供电话支持。

## ☒ 邮件服务

如果您在使用产品过程中，有任何疑问，请发邮件至 [support@colasoft.com.cn](mailto:support@colasoft.com.cn)，我们会在第一时间响应并回复。

## ☒ 备件优先更换服务

对于不在现场服务覆盖范围内的地区或其他不具备现场服务条件的情况，在与您技术确认后，确需更换故障部件的，我们将采用备件优先更换的方式提供服务，备件优先更换服务是指您无需先行将故障产品或部件归还给科来即可获得此故障产品或部件的更换品，备件可能是新品或同类别、性能完好的良品。

## ☒ 1 小时电话响应、2 小时提出解决方案

在免费保修期限内，科来技术支持服务机构将在接到您的报修请求后的 1 个工作日内与您电话联系，确定维修事宜，并在 2 小时内提出解决方案，并在覆盖城市提供第二工作日上门服务，其它城市第三工作日上门服务。

更多售后及服务方式，请参见“科来产品保修服务条款”。

## 2. 技术服务中心

科来软件服务中心电话：400-6869-069

官方网站：<http://www.colasoft.com.cn>

服务邮箱：[support@colasoft.com.cn](mailto:support@colasoft.com.cn)

通信地址：成都市高新区府城大道西段 399 号天府新谷 5 号楼 10 楼

邮编：610041