瑞星2010企业版杀毒软件介绍

之应用技巧和日常维护

2010年11月19日

企业版产品

企业版产品介绍

产品的注册与安装

ID号、序列号、行业信息专用码的用途与区别

管理控制台介绍

个性化全局策略

系统中心与客户端功能介绍

企业版产品安装

- **系统中心的安装**
- **客户（服务器）端的安装**

1. 手动安装
2. 域脚本安装
3. WEB服务器发布安装
4. 中心定制客户端安装包
5. 远程安装（仅限NT内核）

相关演示

企业版产品介绍

系统中心、服务器端、客户端、数据库

系统中心：网络版核心主控系统，负责管理维护服务器端与客户端的信息

必须有固定的IP地址，TCP/IP协议，并且只能安装在服务器端

服务器端：防病毒子系统，针对微软server内核的系统

客户端：防病毒子系统，普通的非server内核系统

数据库：负责存储瑞星产品的日志数据，只需在系统中心安装。

企业版产品优势：采用B/S架构，可实现全网同步杀毒打补丁、全网远程操作，全网远程报警。

产品分类

网络版产品线

- 高级企业专用版：可根据需求定制功能和标题栏，带防火墙
- 高级企业版：可实现跨中心管理，带防火墙
- 企业版：全功能产品（支持多级中心-需两个以上企业版）
- 企业(行业)专用版：可按用户要求定制功能和标题栏
- 教育专用版：不具备漏洞扫描功能，可定制功能和标题栏
- 中小企业版：上限100授权，不可以扩展为多级中心
- 小企业版：没有远程功能，系统中心安装在客户端系统上

产品功能比较一览

功能	高级企业专用版	高级企业版	企业专用版	企业版	教育专用版	中小企业版	小型企业版		
客户端远程安装	可定制	有	可定制	有	可定制	有	**无**		
远程查杀	可定制	有	可定制	有	可定制	有	有		
漏洞扫描	可定制	有	可定制	有	**无**	有	**无**		
广播信息	可定制	有	可定制	有	可定制	有	有		
授权计数的限制	无	无	无	无	无	**有**	**有**		
防火墙功能	**有**	**有**	无	无	无	无	无		
Lotus Notes嵌入式杀毒	可定制	有	可定制	有	可定制	有	**无**		
Office/IE嵌入式杀毒	可定制	有	可定制	有	可定制	有	有		
Outlook嵌入式杀毒	有	有	有	有	有	有	有		
邮件监控	可定制	有	可定制	有	可定制	有	有		
瑞星助手	可定制	有	可定制	有	可定制	有	有		
引导区备份	可定制	有	可定制	有	可定制	有	**无**		

瑞星企业版适用范围

- 对象：各种企业，教育机构，政府机关，网吧等局域网环境；
- 操作系统：包括win7在内的主流windows操作系统以及FreeBSD、UNIX（SUN Solaris系列、IBM AIX系列）、Linux（RedHat Linux、红旗Linux等基于Intel x86芯片的系统）等os；
- 支持语言：中文(简体和繁体)、英文

管理控制台

- 管理控制台是在网络上集中管理所有安装有瑞星杀毒软件网络版客户端软件的计算机的**管理工具**。通过管理控制台可以了解整个网络中的**总体安全状况**并且**远程管理**网络中的任何一台计算机中的瑞星杀毒软件。

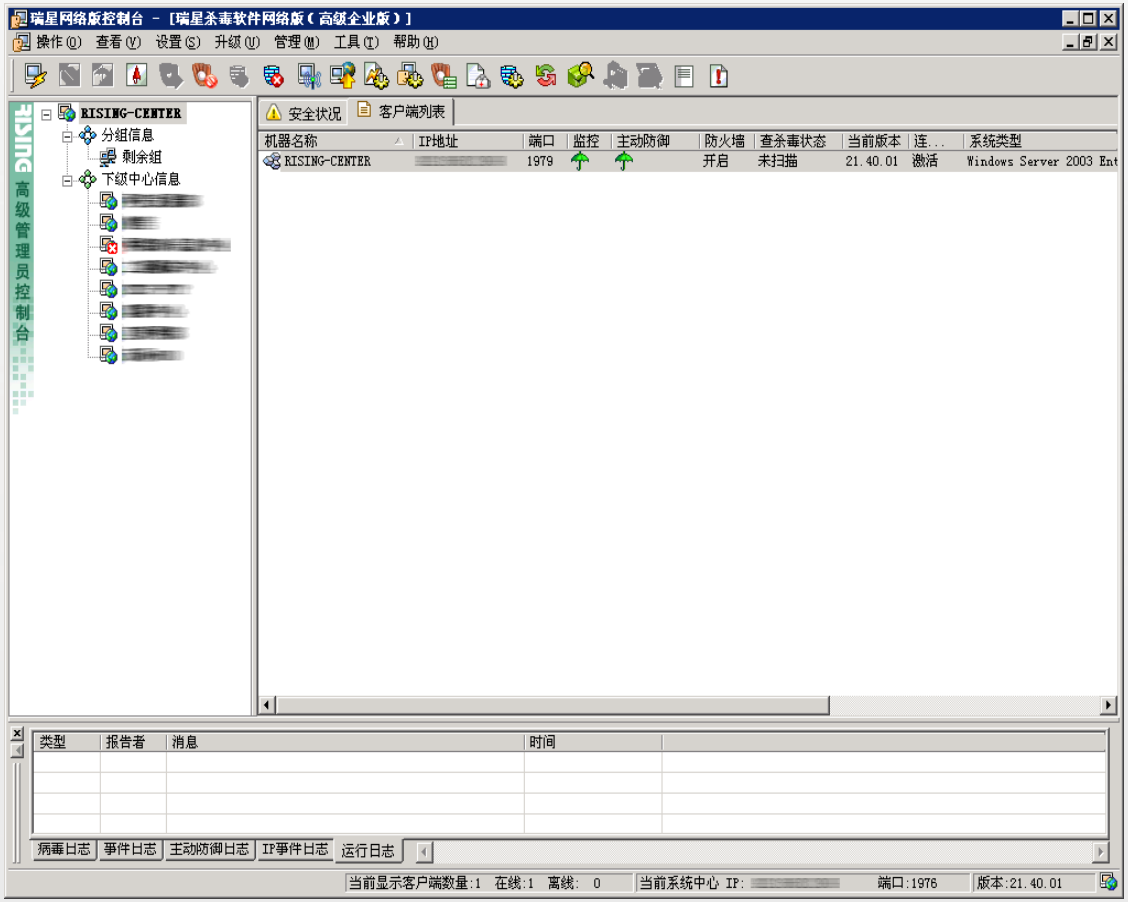
- 网络上任何一台计算机的病毒警告信息都能在管理控制台得到**汇总**，通过管理控制台也能直观地查看网络上所有计算机当前的**实时监控状态**、**病毒查杀情况**、**主动防御状态**和**当前版本信息**等。

- 管理控制台能对**远程计算机安装**瑞星杀毒软件和移动管理控制台，让管理控制台自由移动到管理员认为合适的计算机上去。管理员通过对管理控制台的操作就能对网络上所有计算机进行**定期、实时地查杀病毒**和**全网统一升级管理**，真正做到在整个网络中建立起坚实的网络病毒防护系统。

控制台的登录

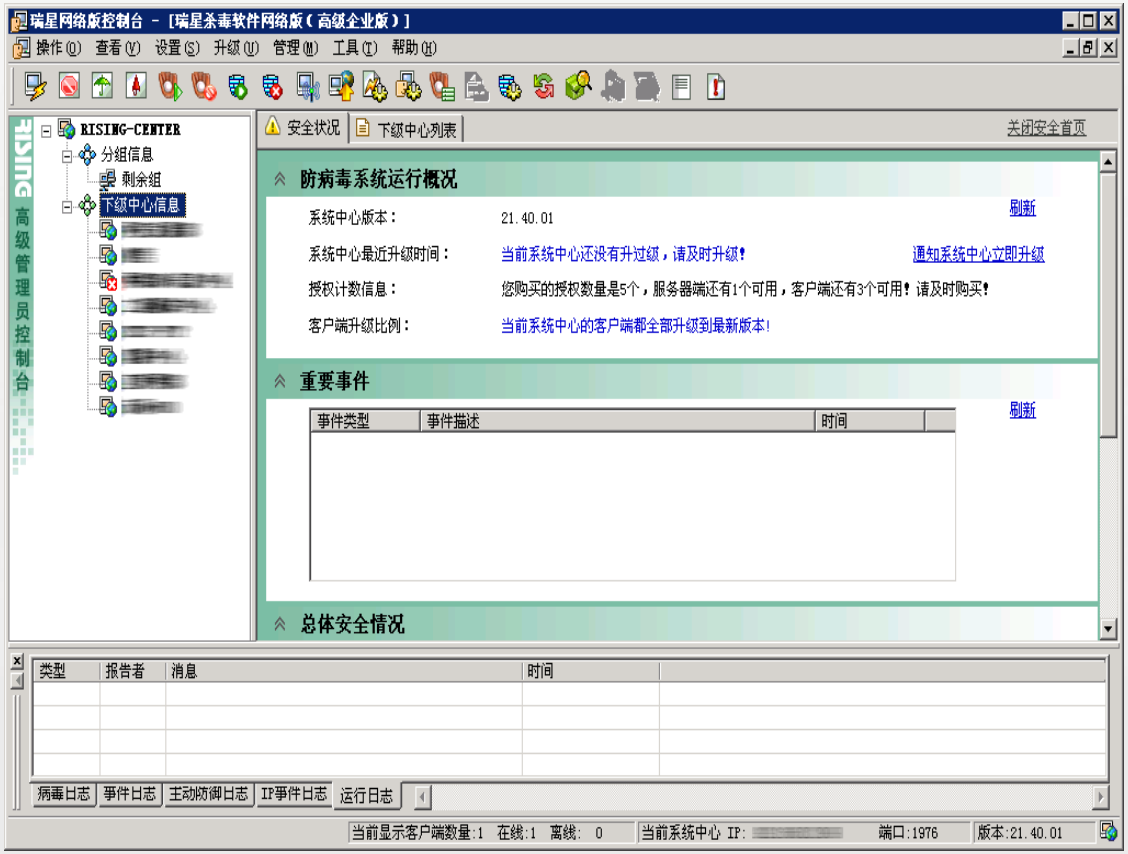
如果控制台密码忘记了怎么办？

控制台主界面



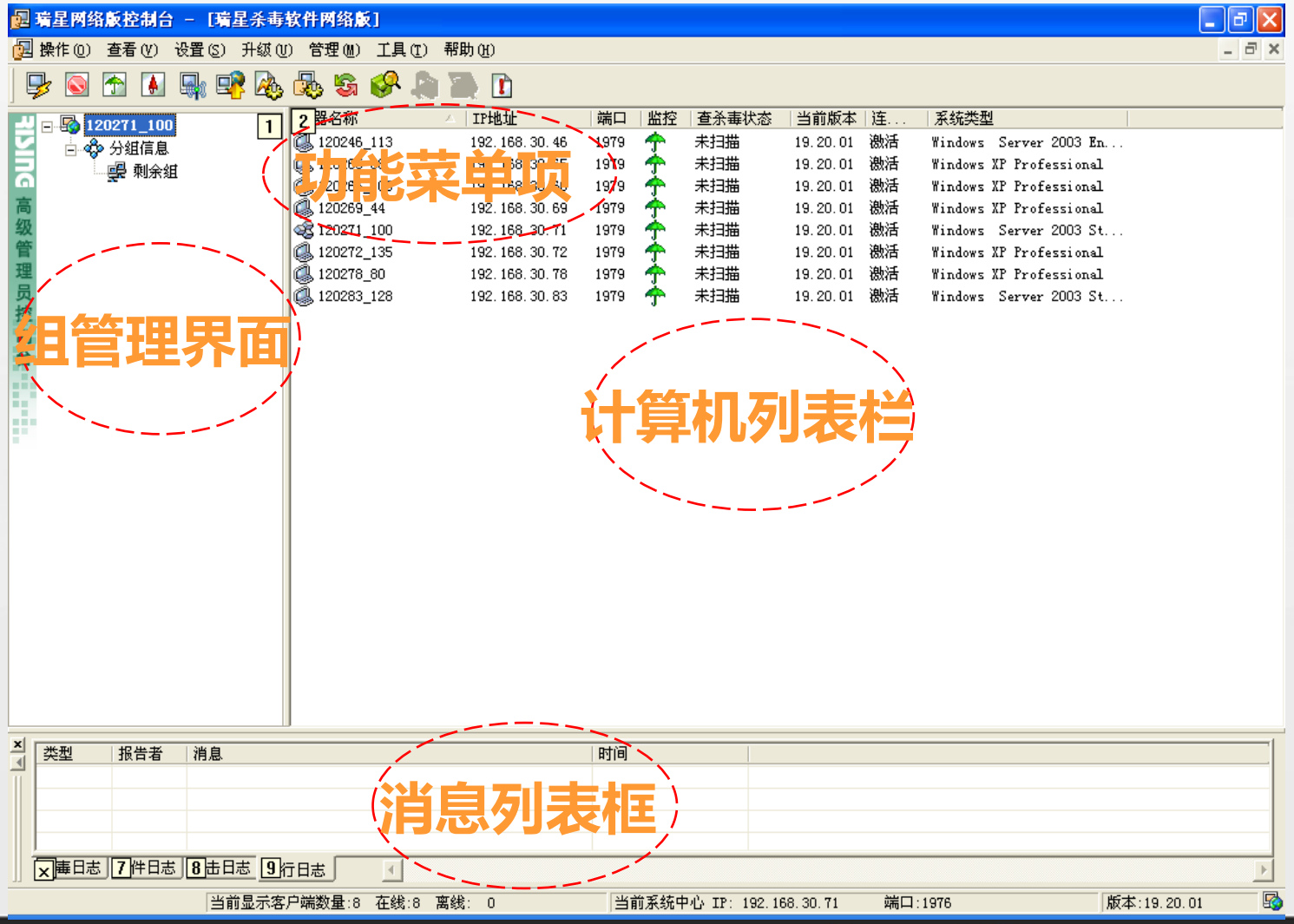
管理控制台界面包括六个部分：菜单、组管理界面、安全状况、客户端列表、日志栏和状态栏。

控制台安全状况界面



管理控制台通过安全状况页面显示本级中心的重要安全状况信息，使得管理员能够全面直观地了解整个网络的安全状况，其中主要内容包括：防病毒系统运行概况、重要事件和总体安全情况。

管理控制台的使用


瑞星网络版控制台 - [瑞星杀毒软件网络版]
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
120271_100
分组信息
剩余组
1
2
机器名称 IP地址 端口 监控 查杀毒状态 当前版本 连... 系统类型
120246_113 192.168.30.46 1979 未扫描 19.20.01 激活 Windows Server 2003 En...
1979 未扫描 19.20.01 激活 Windows XP Professional
1979 未扫描 19.20.01 激活 Windows XP Professional
120269_44 192.168.30.69 1979 未扫描 19.20.01 激活 Windows XP Professional
120271_100 192.168.30.71 1979 未扫描 19.20.01 激活 Windows Server 2003 St...
120272_135 192.168.30.72 1979 未扫描 19.20.01 激活 Windows XP Professional
120278_80 192.168.30.78 1979 未扫描 19.20.01 激活 Windows XP Professional
120283_128 192.168.30.83 1979 未扫描 19.20.01 激活 Windows Server 2003 St...
功能菜单项
组管理界面
计算机列表栏
类型 报告者 消息 时间
消息列表框
毒日志 7件日志 8击日志 9行日志
当前显示客户端数量:8 在线:8 离线: 0
当前系统中心 IP: 192.168.30.71 端口:1976
版本:19.20.01

瑞星网络版的策略设置

利用控制台设置全局策略

1）设置防毒策略

- ◆病毒查杀策略（清除、删除、重启删除）
- ◆开机加载查杀任务（开机、屏保、定时）
- ◆硬盘备份分区表（不推荐使用）

重点：复合文档清除要重启，复合文件指的特定格式的压缩文件，通常由病毒制造者压缩程序使用的外壳

瑞星网络版的策略设置

2）设置客户端选项

◆升级时间（从中心升级的时间）

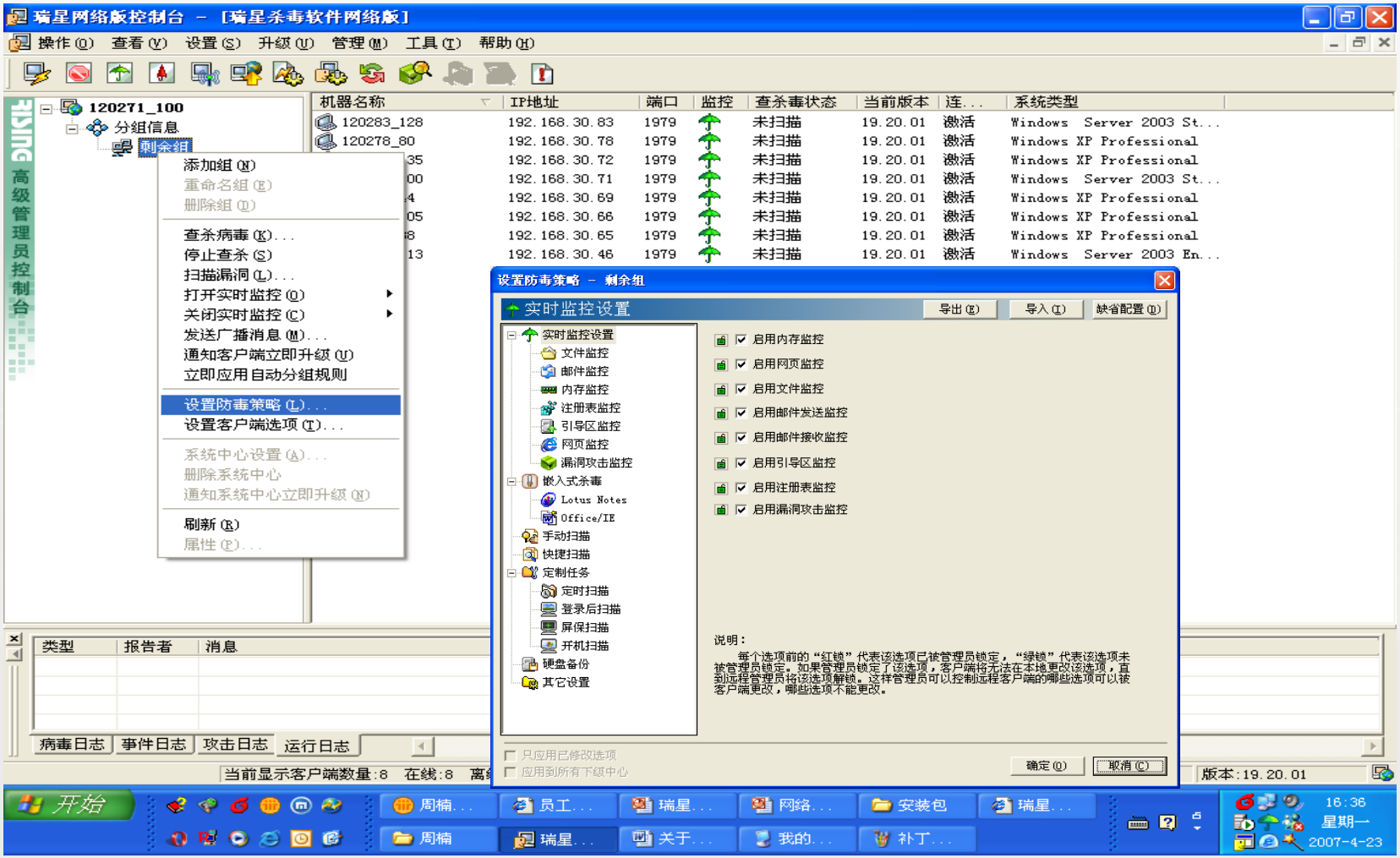
◆密码保护（保证客户端子系统安全）

◆漏洞扫描（设定漏洞扫描的时间）

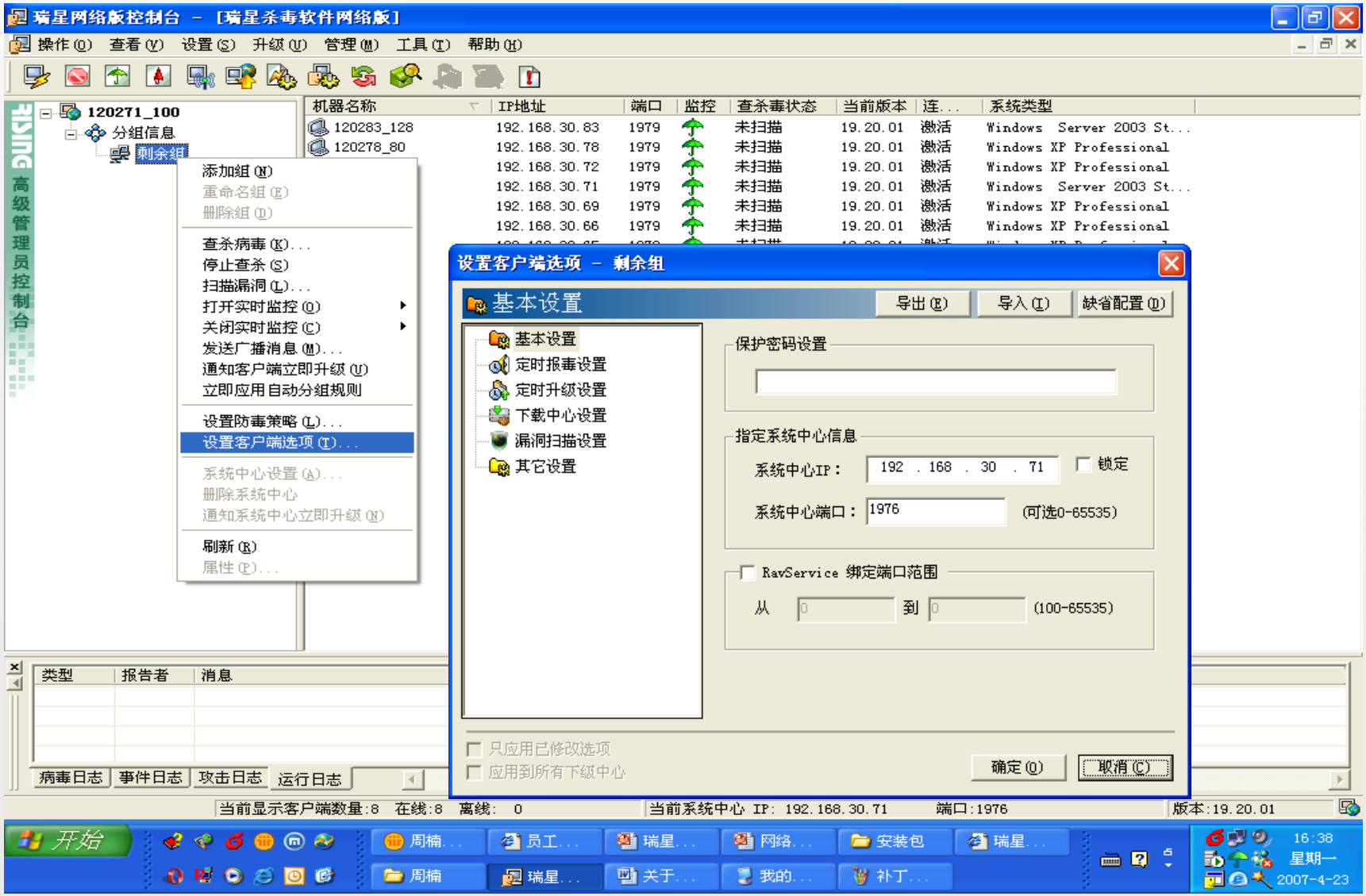
◆代理设置（指定代理升级中心的IP）

重点：密码保护，不要与控制台登录密码混淆

瑞星网络版的策略设置


瑞星网络版控制台 – [瑞星杀毒软件网络版]
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
120271_100
分组信息
剩余组
添加组(N)
重命名组(E)
删除组(D)
查杀病毒(K)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
发送广播消息(M)...
通知客户端立即升级(U)
立即应用自动分组规则
设置防毒策略(L)...
设置客户端选项(T)...
系统中心设置(A)...
删除系统中心
通知系统中心立即升级(N)
刷新(R)
属性(P)...
机器名称 IP地址 端口 监控 查杀毒状态 当前版本 连... 系统类型
120283_128 192.168.30.83 1979 未扫描 19.20.01 激活 Windows Server 2003 St...
120278_80 192.168.30.78 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.72 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.71 1979 未扫描 19.20.01 激活 Windows Server 2003 St...
192.168.30.69 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.66 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.65 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.46 1979 未扫描 19.20.01 激活 Windows Server 2003 En...
设置防毒策略 – 剩余组
实时监控设置
导出(E) 导入(I) 缺省配置(D)
实时监控设置
文件监控
邮件监控
内存监控
注册表监控
引导区监控
网页监控
漏洞攻击监控
嵌入式杀毒
Lotus Notes
Office/IE
手动扫描
快捷扫描
定制任务
定时扫描
登录后扫描
屏保扫描
开机扫描
硬盘备份
其它设置
启用内存监控
启用网页监控
启用文件监控
启用邮件发送监控
启用邮件接收监控
启用引导区监控
启用注册表监控
启用漏洞攻击监控
说明：
每个选项前的“红锁”代表该选项已被管理员锁定，“绿锁”代表该选项未被管理员锁定。如果管理员锁定了该选项，客户端将无法在本地更改该选项，直到远程管理员将该选项解锁。这样管理员可以控制远程客户端的哪些选项可以被客户端更改，哪些选项不能更改。
只应用已修改选项
应用到所有下级中心
确定(O) 取消(C)
类型 报告者 消息
病毒日志 事件日志 攻击日志 运行日志
当前显示客户端数量:8 在线:8
版本:19.20.01
开始
周楠... 员工... 瑞星... 网络... 安装包 瑞星...
周楠 瑞星... 关于... 我的... 补丁...
16:36
星期一
2007-4-23

瑞星网络版的策略设置


瑞星网络版控制台 – [瑞星杀毒软件网络版]
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
120271_100
分组信息
剩余组
添加组(N)
重命名组(E)
删除组(D)
查杀病毒(K)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
发送广播消息(M)...
通知客户端立即升级(U)
立即应用自动分组规则
设置防毒策略(L)...
设置客户端选项(T)...
系统中心设置(A)...
删除系统中心
通知系统中心立即升级(N)
刷新(R)
属性(P)...
机器名称 IP地址 端口 监控 查杀毒状态 当前版本 连... 系统类型
120283_128 192.168.30.83 1979 未扫描 19.20.01 激活 Windows Server 2003 St...
120278_80 192.168.30.78 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.72 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.71 1979 未扫描 19.20.01 激活 Windows Server 2003 St...
192.168.30.69 1979 未扫描 19.20.01 激活 Windows XP Professional
192.168.30.66 1979 未扫描 19.20.01 激活 Windows XP Professional
设置客户端选项 – 剩余组
基本设置
导出(E) 导入(I) 缺省配置(D)
基本设置
定时报毒设置
定时升级设置
下载中心设置
漏洞扫描设置
其它设置
保护密码设置
指定系统中心信息
系统中心IP: 192 . 168 . 30 . 71 锁定
系统中心端口: 1976 (可选0-65535)
RavService 绑定端口范围
从 0 到 0 (100-65535)
只应用已修改选项
应用到所有下级中心
确定(O) 取消(C)
类型 报告者 消息
病毒日志 事件日志 攻击日志 运行日志
当前显示客户端数量:8 在线:8 离线: 0
当前系统中心 IP: 192.168.30.71 端口:1976
版本:19.20.01
开始
16:38
星期一
2007-4-23

漏洞扫描功能

在**企业专用版**和**高级企业专用版**中，购买时可以**定制**该功能；**中小企业版、企业版**和**高级企业版**中有该功能。

在管理控制台上可以任选一台或多台计算机进行漏洞扫描。管理员可以通过立即执行漏洞扫描的方式，及时的了解客户端漏洞情况。

用户可以在【扫描系统漏洞】和【扫描不安全设置】选项前的复选框中勾选或取消勾选，扫描后会根据用户的选择显示相应的扫描信息。

用户可以选择【严重级别】对系统漏洞和不安全设置进行扫描，分为全部、最高、中级以上、低级以上四种，用户可根据需求设置扫描级别。

漏洞扫描

如何通过控制台进行漏洞扫描

如何开启漏洞扫描

漏洞扫描界面如何进入

如何自动安装扫描出的漏洞补丁

如何导入其它机器下载的补丁

如何在非涉密机器上下载补丁程序

相关演示

升级功能

系统中心升级方式

升级中心有以下3种方式升级
1.从上级中心升级
2.从网站升级
下载需要更新的文件升级
下载手动安装包升级
3.自动升级（先从上级中心，在从网站）
其实上面3种升级方式严格来说，可认为是2种升级方式，因为自动升级方式，只不过是第一种、第二种一种组合方式。

升级功能

客户端升级方式

1.客户端从系统中心升级。这是网络版的传统升级方式。

2.客户端从本级中心获取升级代理信息，从代理升级。

3.游离升级，网络版移动设备（笔记本）在不能连接中心且开启游离功能的情况下，直接从网站升级。该功能是09网络版新增的一个功能。

升级功能

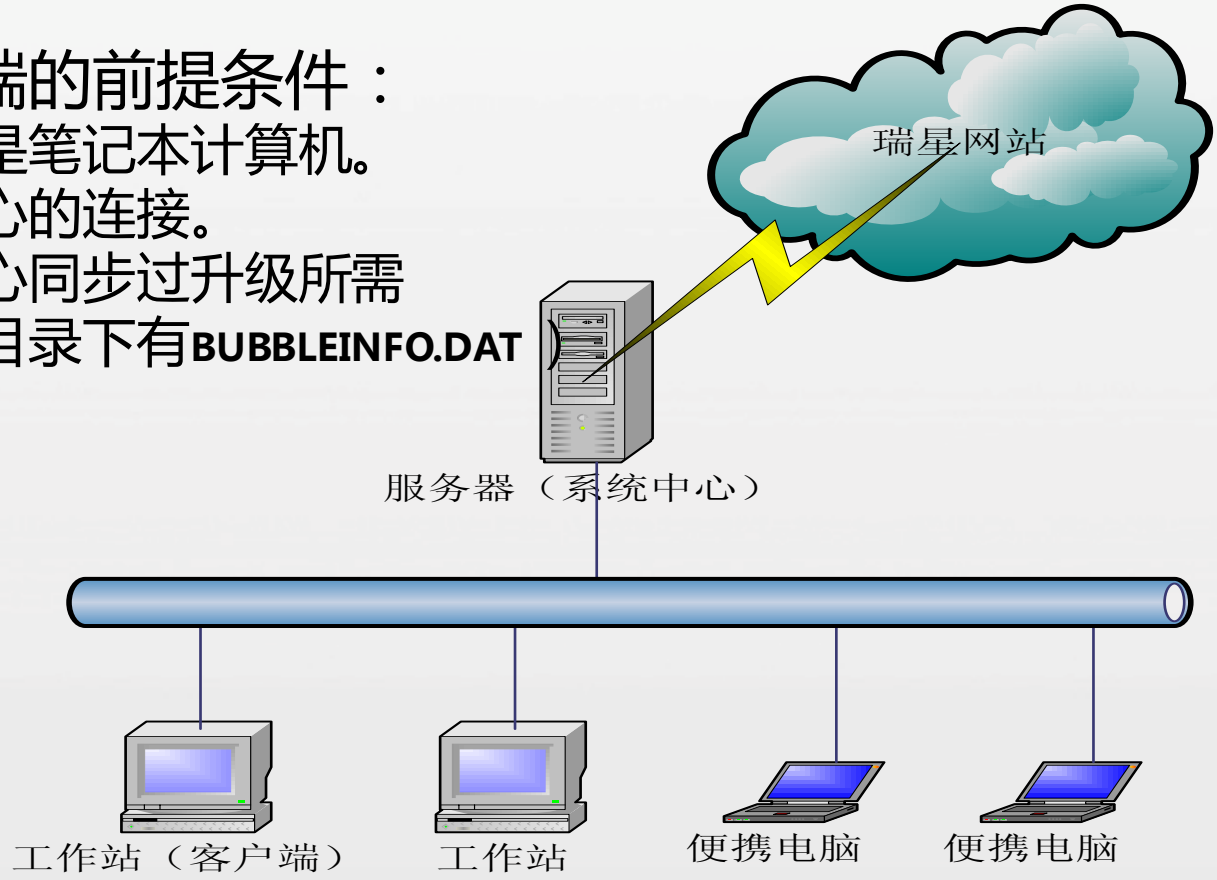
游离升级功能介绍

客户端成为游离客户端的前提条件：

该客户端主机必须是笔记本计算机。

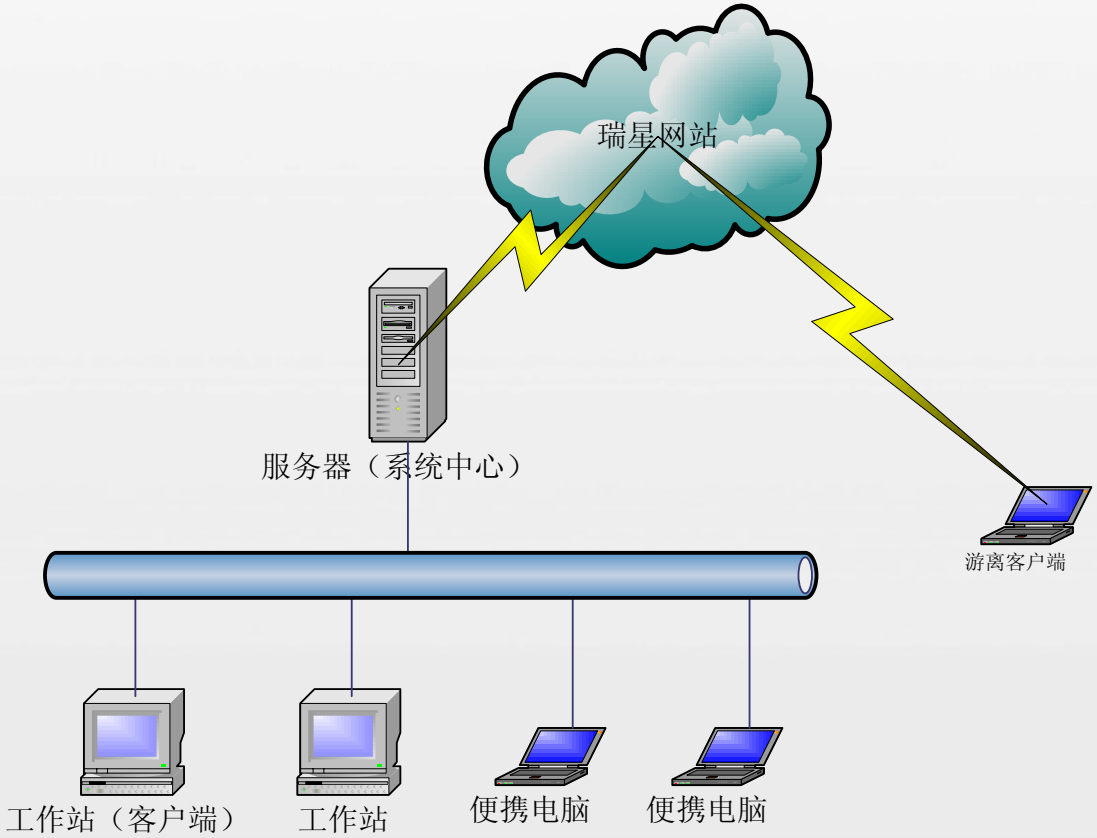
必须断开与系统中心的连接。

必须成功从系统中心同步过升级所需的游离信息（安装目录下有**BUBBLEINFO.DAT**



升级功能

游离升级功能介绍



当客户端脱离系统中心处于游离状态时，只要其能够连接互联网，就能够从瑞星网站更新最新的病毒库和程序，使它能够得到最大限度的保护。

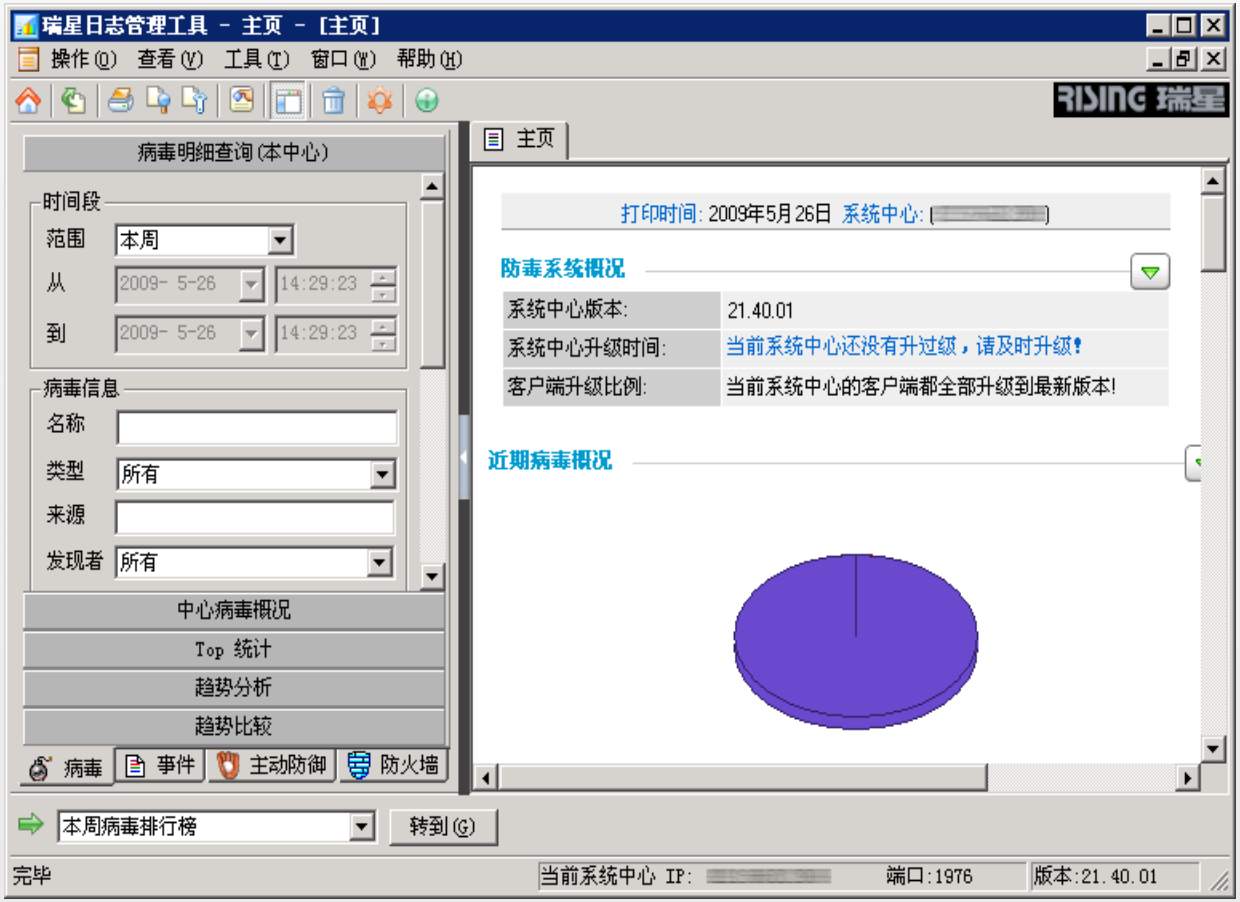
瑞星日志管理

日志管理功能介绍

- 通过瑞星日志管理工具，管理员可对病毒、事件、主动防御和防火墙的日志进行查询统计。
- 瑞星日志管理工具可以以不同种类的帐号登陆，超级管理员对瑞星日志管理工具有完全的操作权限，而以操作管理员或审计管理员帐号登录此工具时，对于工具中的【日志删除】和【计划任务管理】都没有权限使用。
- 瑞星日志管理，包括【病毒】、【事件】、【主动防御】和【防火墙】四大项，可以选择查询不同类型的日志信息。日志查询统计工具就会给用户最清晰的结果显示。

瑞星日志管理

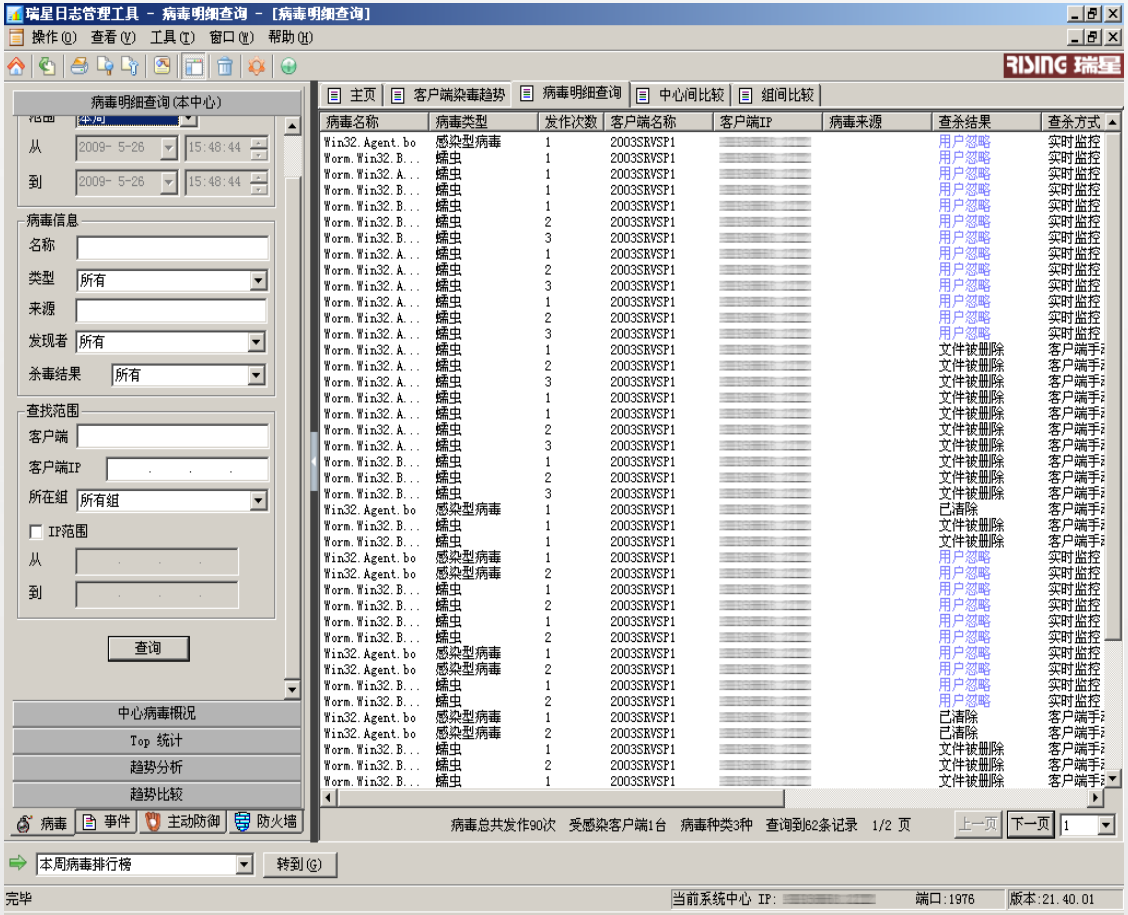
日志管理功能介绍



瑞星日志管理工具界面的左侧是项目栏，包括【病毒】、【事件】、【主动防御】和【防火墙】四个标签页，可以选择查询不同类型的日志信息。

瑞星日志管理

日志管理功能介绍



病毒日志的管理共包括五部分：【病毒明细查询（本中心）】、【中心病毒概况】、【Top统计】、【趋势分析】和【趋势比较】。

日志常见“关键词”说明

- “用户忽略”：该提示是指在控制台下发全网查杀策略时，没有设置客户端保护密码的情况下，用户自行停止了杀毒软件的查杀行为。（注：该操作会提升局域网病毒威胁，建议谨慎操作）
- “已清除”：该提示是指在客户端杀毒过程中，已经成功的清除病毒。（注：与“文件被删除”提示有区分）
- “重启后删除”：该提示是当某些病毒程序挂载在当前运行的程序上，无法直接停止其应用，所以需要重新启动计算机时删除。
- “删除失败”：该提示是指某些顽固病毒，无法通过杀毒软件清除，只能进行手动清除。（注：这种情况并非和杀毒软件的查杀能力相关，而是病毒本身设置的较高的操作权限，正规的杀毒软件无法达到）
- “复合文档回写失败”：该提示与查杀方式是相关的，是指杀毒软件在提取染毒文件中的病毒进行清除之后，无法将文件本身的内容完全回写进去，构成了一定的数据损坏。

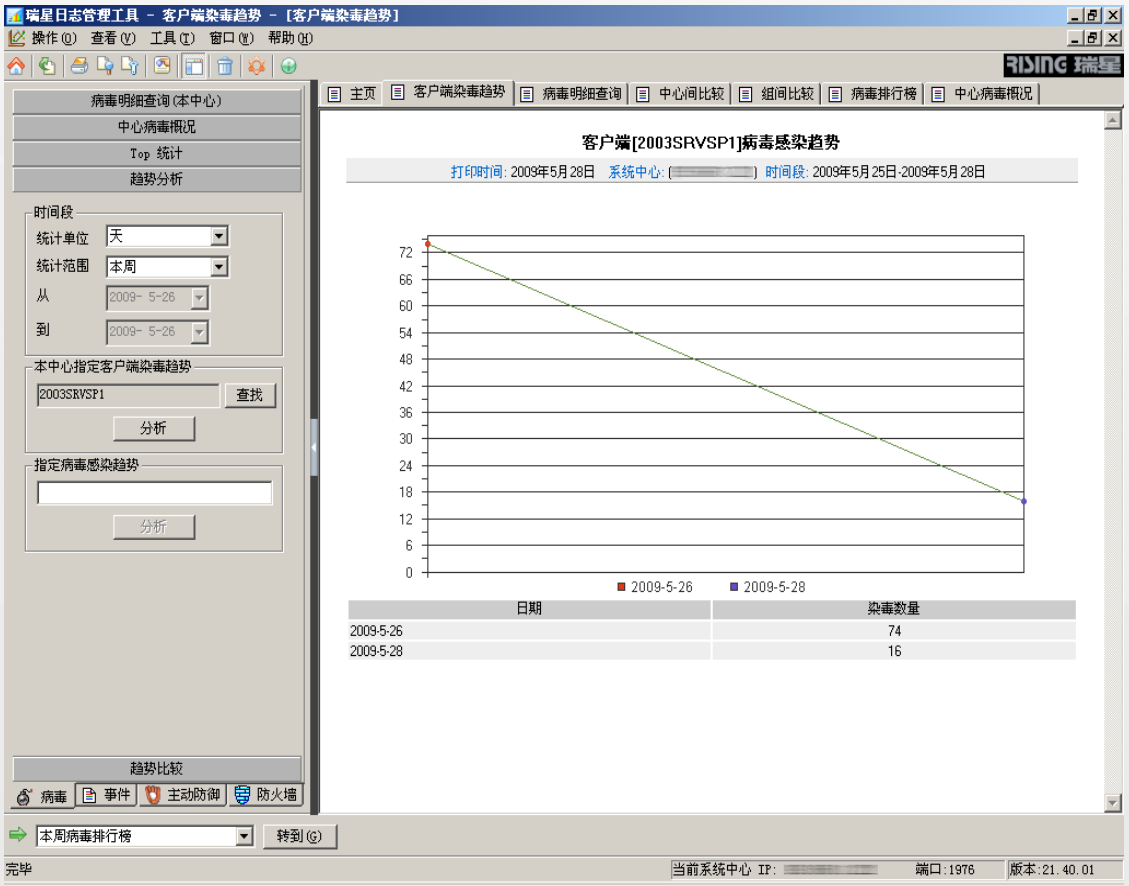
瑞星日志管理

日志管理功能介绍

用户通过【Top统计】功能，可以查询病毒排行、本中心客户端排行、本中心组排行和中心排行，选择要统计的内容后，单击【统计】按钮后，显示统计结果

瑞星日志管理

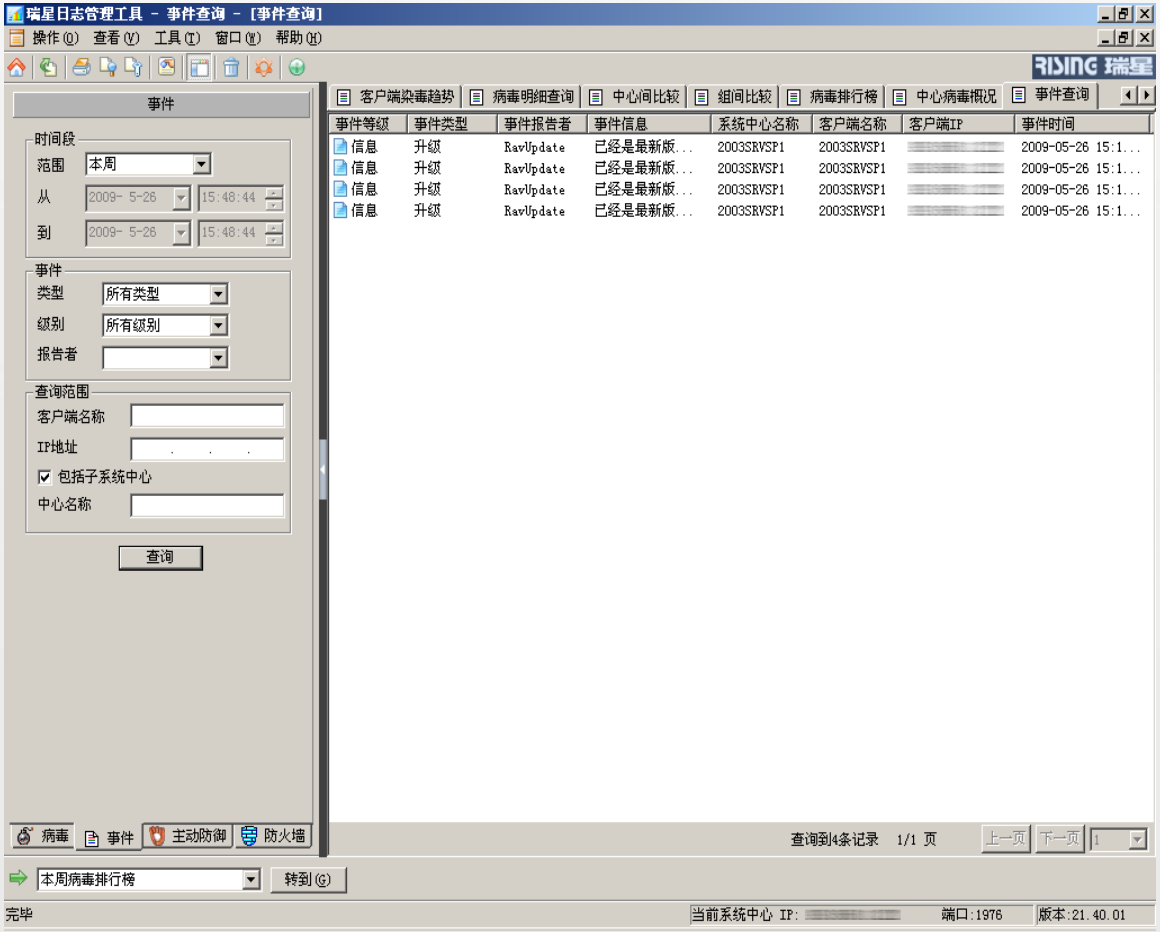
日志管理功能介绍



【趋势分析】功能提供分析某一时间段内某一客户端或病毒的染毒趋势，及时的预防病毒的侵害。以本周某一客户端病毒感染趋势为例，输入限定条件后单击【分析】按钮后，显示趋势图

瑞星日志管理

日志管理功能介绍



瑞星日志管理工具可以对事件日志进行查询，在左面的查询栏中输入查询条件后，单击【查询】按钮即可显示查询结果。

瑞星日志管理

日志管理功能介绍

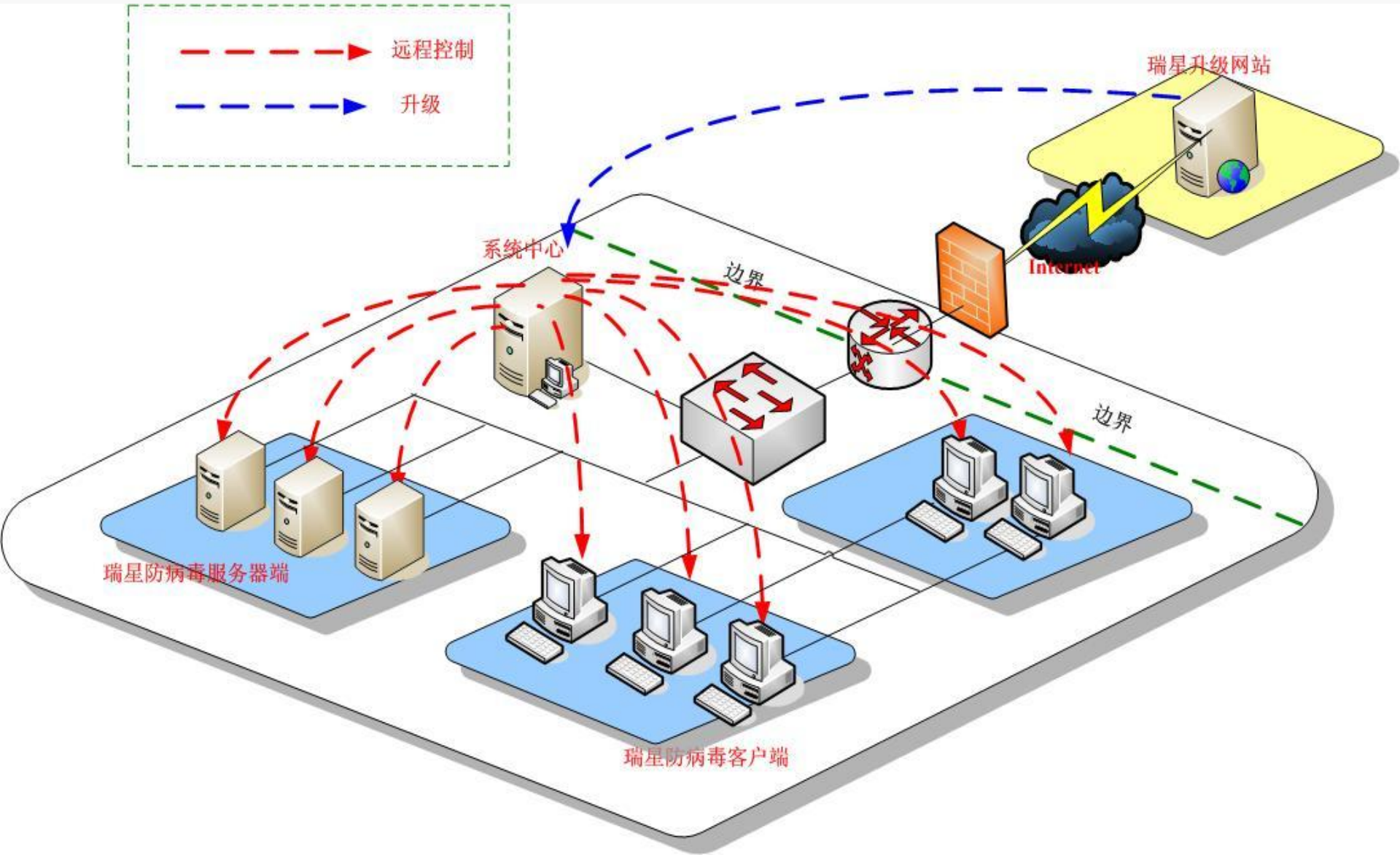
- 网络版对于病毒详细日志，不提供多级查询，中心只能查询到本级的病毒详细日志
- 一级中心可以查询所属二级中心的病毒统计日志
- 一级中心可以查询所属二级中心的事件日志
- 一级中心可以查询所属二级中心的防火墙日志
- 主动防御日志，只能在本级中心查询

服务器和客户端所需要开放的端口

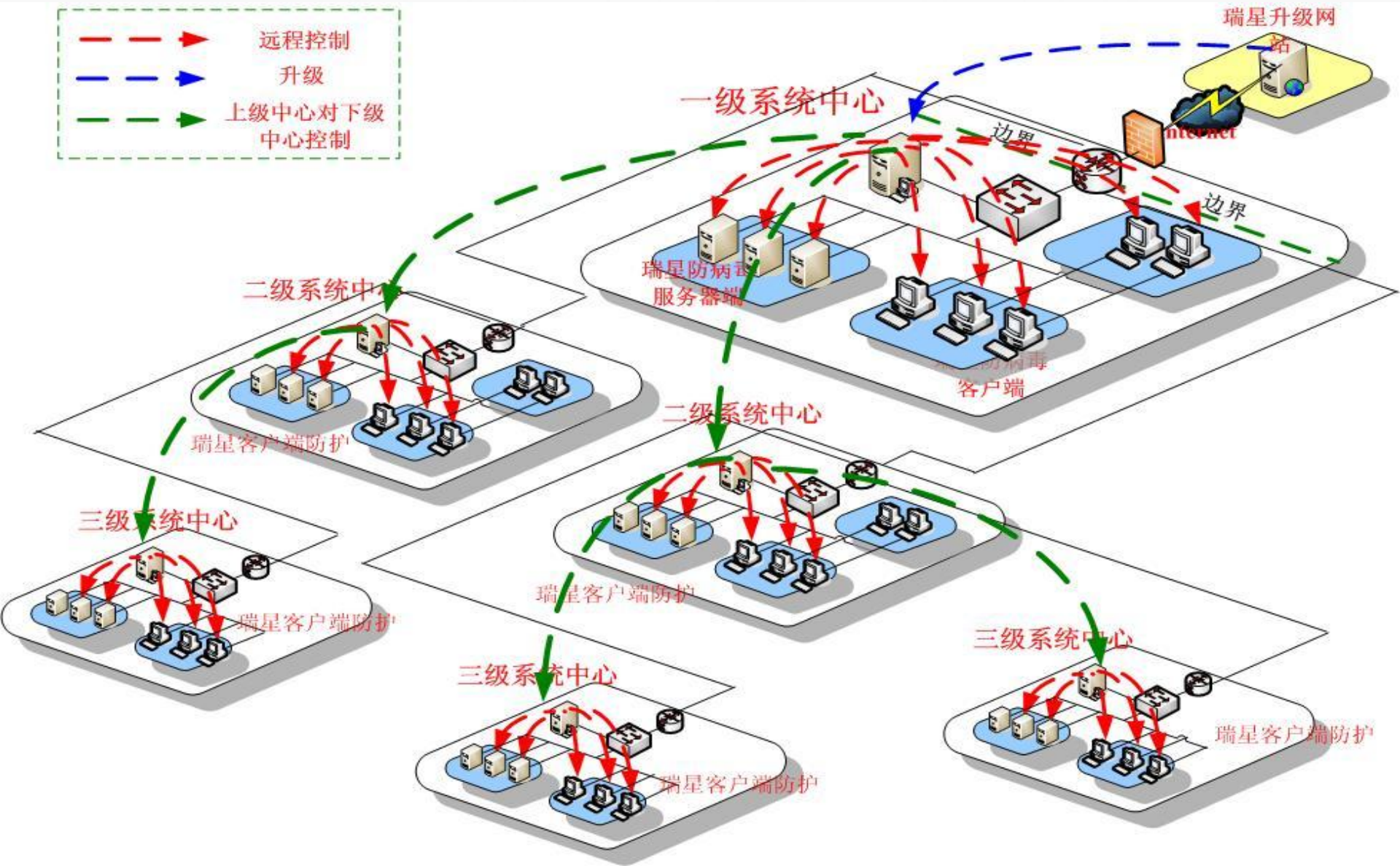
- 在服务器正常运行的时候需要保证以下计算机端口开放：

- TCP/IP：
  - 1976端口 —— RAVagent——主要负责系统中心数据的管理
  - 1977端口 —— RAVupdate—主要负责中心及客户端的升级
  - 1978端口 —— RAV net alert——主要负责系统中心的警报服务
  - 1979端口 —— RAVservice——主要负责客户端（服务器端）的通讯
  - 1980端口 —— RNreport——主要负责系统中心的查询统计服务
  - 1981端口 —— RAVcontrol——控制台所需服务
  - 1982端口 —— RAVupgrd——升级组件
  - 1983端口 —— leakmgr.exe——漏洞管理服务
- UDP：
  - 7273——7282端口

常见网络环境部署(单级中心)



常见网络环境部署(多级中心)




谢谢大家