重要声明

感谢您购买瑞星公司出品的瑞星虚拟化系统安全软件系列产品。请在使用瑞星虚拟化系统安全软件之前认真阅读配套的使用手册，当您开始使用瑞星虚拟化系统安全软件时，瑞星公司认为您已经阅读了本使用手册。

本使用手册的内容将随着瑞星虚拟化系统安全软件的更新而改变，恕不另行通知。从瑞星网站（www.rising.com.cn）可下载本使用手册的最新版。因使用手册对用户可能产生的影响，瑞星公司不承担责任。

瑞星虚拟化系统安全软件产品均可以通过瑞星网站使用序列号在线注册。注册后的产品才会得到唯一合法使用该套产品的“服务号”，用户根据服务号和注册设置的密码再次登录网站，可以申请产品授权证书并以电子邮件方式发送。对于自购买日起一个月后未持有“产品授权书”的使用者，瑞星公司有权拒绝提供升级程序、技术支持和售后服务，并对因未及时获得瑞星公司的产品、技术、病毒疫情和服务等信息而造成的影响不承担任何责任。了解注册用户获得的服务，请参阅《客户服务指南》。

作为系统安全产品，瑞星虚拟化系统安全软件将进行不断的升级。无论是功能的增加、性能的提高还是清除病毒种类的增加，都关系到其实际的使用价值。所以，在使用本产品过程中应随时保持与瑞星公司的联系，以便及时获得升级程序或更新换代产品。

忠告用户

（1）请将所购产品与“产品组件清单”进行核对，以确定产品的完整性。确认购买的产品为瑞星公司的正版产品；

（2）如果自购买日起一个月后未注册，将不能得到包括升级在内的技术支持和售后服务；

（3）为了避免“产品序列号”、“授权证书”等机密信息泄露，保障用户的合法权益不受侵害，瑞星公司不接受除了最终用户以外的任何人或机构的代替注册；

（4）请准确填写注册中的每项内容并及时注册；

（5）请妥善保管“产品序列号”和“授权证书”，以免软件被盗用，从而影响自己的正常使用；

（6）如对产品包装内物品和注册过程有疑义，请立即向该套产品的提供商或瑞星公司咨询；

（7）任何情况下，不得在授权范围外使用本软件。

瑞星客户服务联系方式

如果遇到了问题，在您寻求技术支持之前，请务必先仔细阅读本使用手册，或者直接访问瑞星网站中的客户服务频道寻找您遇到的问题和解决办法，我们将尽力帮助您解决问题。若您所遇到的问题仍然没有解决，请发送电子邮件或拨打瑞星公司客户服务电话。

客户服务：010-82678800（自费电话）　　400-660-8866（免长途话费）

邮件服务中心：http://mailcenter.rising.com.cn

网址：http://www.rising.com.cn

邮政编码：100190

通信地址：北京市海淀区中关村大街 22 号中科大厦 1408 室

2013 年 8 月 北京 • 中国

目录

第一章 软件产品说明

1.1 产品组成

当您通过合法途径获得瑞星虚拟化系统安全软件的使用权后，在安装使用前，请仔细检查核对包装内的《产品组件清单》。

1. 光盘：包含用户所购买的瑞星虚拟化系统安全软件所有程序。
2. 《使用手册》：即本手册，通过阅读它，掌握本软件的详细使用方法和技巧。
3. 《客户服务指南》：该指南将帮助用户获取技术支持和服务方面的信息。
4. 《快速安装指南》：指导用户快速掌握软件安装的方法。
5. 产品序列号：为本套产品分配的唯一身份证明，缺少它，本软件将无法安装。（注意：产品序列号见本手册封二）。
6. 《产品组件清单》：用于核对产品组件，以确定产品的完整性。
7. 《功能快速查阅表》：了解产品主要功能，帮助用户快速查阅“使用手册”中相关功能的详细描述。
8. 《注册扩容指南》：该指南详细介绍了购买本产品后如何进行产品注册和产品扩容。

1.2 应用环境

1.2.1 管理中心

a. 软件环境

（1）操作系统

Windows 2003 Server SP2（32-bit、64-bit）

Windows Server 2008（32-bit、64-bit）

Windows Server 2008 R2（64-bit）

（2）其它

Web 服务器：IIS 6.0 以上

数据库：MySQL 5.0 以上

浏览器：Microsoft Internet Explorer 8 以上、Firefox、Google Chrome、Safari

b. 硬件和网络要求

CPU：800MHz 以上

内存：4GB

硬盘空间：5GB

网络环境：100M 以上网络，需一个固定 IP 地址

1.2.2 安全虚拟设备

a. 软件环境

（1）操作系统

VMware vCenter 4.0.0 及以上

ESXi 5.0.0、5.1.0

（2）其它

额外的 VMware 工具：VMware Tools、VMware vShield Manager、 VMware vShield Endpoint Security 5.0（ESXi5 patch ESXi500-201109001 for vShield Endpoint Driver）

VMware Endpoint Protection 支持的操作系统：Windows XP SP2（32-bit）、Windows 2003 SP2（32-bit、64-bit）、Windows Vista（32-bit）、Windows 7（32-bit）、Windows 2008（32-bit、64-bit）。（对于最新支持的客户机平台请参考 VMware 文档）

b. 硬件和网络要求

CPU：64-bit，Intel-VT present and enabled in BIOS

支持的 vSwitch：standard vSwitch 标准虚拟机交换机或第三方 vSwitch 虚拟交换机 –Cisco Nexus 1000v

内存：2GB，内存容量需求取决于 SVM 保护的虚拟机数量

硬盘空间：20GB

1.2.3 日志中心

a. 软件环境

（1）操作系统

Windows 2000 (32-bit)

建议以下系统：

Windows XP SP2（32-bit、64-bit）

Windows 2003 SP2（32-bit、64-bit）

Windows Vista（32-bit、64-bit）

Windows 2008（32-bit、64-bit）

Windows2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：800MHz 以上

内存：512MB 以上

磁盘空间：1GB 以上

1.2.4 升级中心

a. 软件环境

（1）操作系统

Windows 2000 (32-bit)

建议以下系统：

Windows XP SP2（32-bit、64-bit）

Windows 2003 SP2（32-bit、64-bit）

Windows Vista（32-bit、64-bit）

Windows 2008（32-bit、64-bit）

Windows2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：800MHz 以上

内存：512MB 以上

磁盘空间：1GB 以上

1.2.5 查杀协作

a. 软件环境

（1）操作系统

Windows 2000 (32-bit)

建议以下系统：

Windows XP SP2（32-bit、64-bit）

Windows 2003 SP2（32-bit、64-bit）

Windows Vista（32-bit、64-bit）

Windows 2008（32-bit、64-bit）

Windows2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：800MHz 以上

内存：256MB 以上

硬盘空间：500MB 以上

第二章 软件概述

瑞星虚拟化系统安全软件完整防护体系由相互关联的子系统组成，每个子系统均包括若干不同的模块，除承担各自的任务外，还与其它子系统通讯，协同工作，共同完成对虚拟化系统的安全防护。

2.1 管理中心

瑞星虚拟化系统安全软件管理中心是一个强大的基于 Web 的集中式管理系统，管理员可以通过它来创建和管理全面的安全策略，跟踪威胁并记录针对这些威胁所采取的预防处理措施。管理中心支持与用户其他管理系统（包括 VMware vCenter 和 Microsoft Active Directory）通过 Web 服务 API 进行集成。

安全配置文件

安全配置文件是策略模板，用于指定一个或多个客户虚拟机自动配置和执行的安全规则。管理员通过安全配置文件进行安全规则的管理和下发，轻松实现业务环境的全面防护。同时，管理中心缺省提供大量包含常用计算机安全规则的安全配置文件，可以直接应用，进一步简化了安全管理操作。

管理控制台

管理控制台采用可定制的、基于 Web 的界面交互方式，安全管理员可轻松、快速的导航至特定信息并进行详细分析。

控制台支持的主要功能包括：

全面的系统日志（警报、事件、扫描记录等）展示与图表分析；

客户虚拟机安全配置与管理；

自定义个性化版面配置；

与 VMware vCenter、Microsoft Active Directory 等管理系统的联动与集成。

内建安全

基于角色的用户管理，支持设置不同权限层级用户的访问和编辑权限集合，控制用户可以操作和查看的功能信息，避免因非授权人员使用引发的安全风险；

数字签名用于认证系统组件并验证规则的完整性；

会话加密可保护在组件之间交换信息的机密性。

2.2 安全虚拟设备

瑞星虚拟化系统安全软件安全虚拟设备作为 VMware 虚拟机运行，并保护同一 ESXi Server 上的其他虚拟机，且每个安全虚拟设备均拥有各自的安全策略。

病毒防护

瑞星虚拟化系统安全软件与 VMware vShield Manager Endpoint Security 集成，提供病毒安全防护功能。

安全虚拟设备检测到病毒时，可以生成警报，当被保护客户虚拟机安装有查杀协作组件时，能够实现虚拟化系统内部完整的病毒阻止处理措施，包括清除、删除、拒绝访问或隔离等。

2.3 日志中心

瑞星虚拟化系统安全软件日志中心收集各子系统上报的警报、事件、杀毒、升级等日志记录，进行集中管理。系统支持部署多个日志中心实现负载均衡，以应对大数据量日志的上报存储。

2.4 升级中心

瑞星虚拟化系统安全软件升级中心自瑞星官网下载最新版本的更新文件，为管理中心、安全虚拟设备、查杀协作及其自身组件提供更新源，各个子系统自升级中心文件下载服务获取最新文件，完成升级。瑞星虚拟化系统安全软件支持升级中心多级分层结构，且对分层级数没有限制，可以实现升级任务的负载均衡，提高产品升级效率。

2.5 查杀协作

瑞星虚拟化系统安全软件杀毒协作是轻量化高性能组件，可选安装在被保护的客户虚拟机上，配合安全虚拟设备实现完整的杀毒及后处理操作。

第三章 安装与卸载

瑞星虚拟化系统安全软件的基本安装对象包括管理中心、日志中心、升级中心和查杀协作。典型安装时建议先在物理计算机上安装管理中心，然后在其它物理或虚拟机上安装其他对象。

3.1 安装准备

3.1.1 通信端口

瑞星虚拟化系统安全软件需要开放以下默认端口的访问权限：

管理中心

- 管理：29443
- 通信：29121
- 其他：29080

升级中心

- 通信：29088

日志中心

- 通信：29086

MySQL 数据库

- 通信：3306

3.1.2 产品序列号

购买瑞星虚拟化系统安全软件时，您会获到一个产品序列号，使用产品序列号到瑞星公司官方网站注册生成服务号，再使用服务号登陆官方网站获取产品授权证书，授权证书将以电子邮件方式发送至您在网站登记的邮箱。如果没有产品序列号和授权证书，将无法使用产品的安全防护功能。

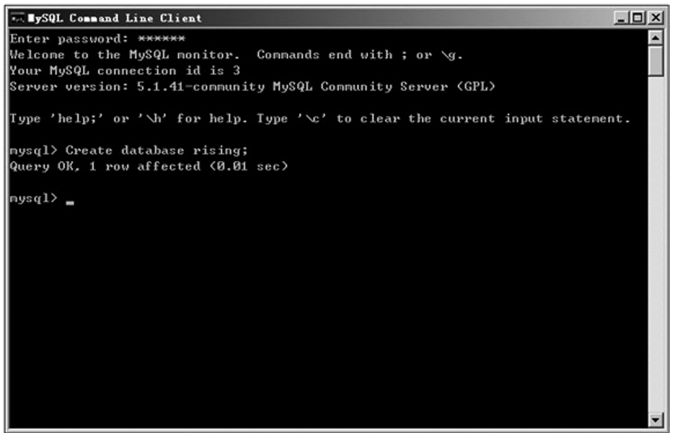
提示：您还需要获取 VMware 相关组件的激活码，如使用瑞星虚拟化系统安全软件杀毒功能必须获得 VMware vShield Endpoint Security 5.0 激活号。

3.1.3 网络连接

瑞星虚拟化系统安全软件各子系统之间的通信是通过主机名或 IP 地址完成，所以要保证管理中心、安全虚拟设备、日志中心、升级中心和客户虚拟机的主机名或 IP 地址能正常通信。

3.1.4 数据库

在部署瑞星虚拟化系统安全软件管理中心与日志中心时，需要安装 MySQL 数据库软件。如果选择安装独立的 MySQL 数据库，需要在数据库管理控制台中预先手动建立数据库实例。例如建立名称为 rising 的数据库，在 MySQL 管理控制台界面输入“Create database rising；”。



图表 3-1

3.1.5 VMware 环境

瑞星虚拟化系统安全软件安全虚拟设备部署需要提供如下 VMware 环境：

VMware vCenter 4.0.0 或以上；

ESXi 5.0.0 或 5.1.0；

额外的 VMware 工具：VMware Tools、VMware vShield Manager、VMware vShield Endpoint Security 5.0（ESXi5 patch ESXi500-201109001 for vShield Endpoint Driver）。

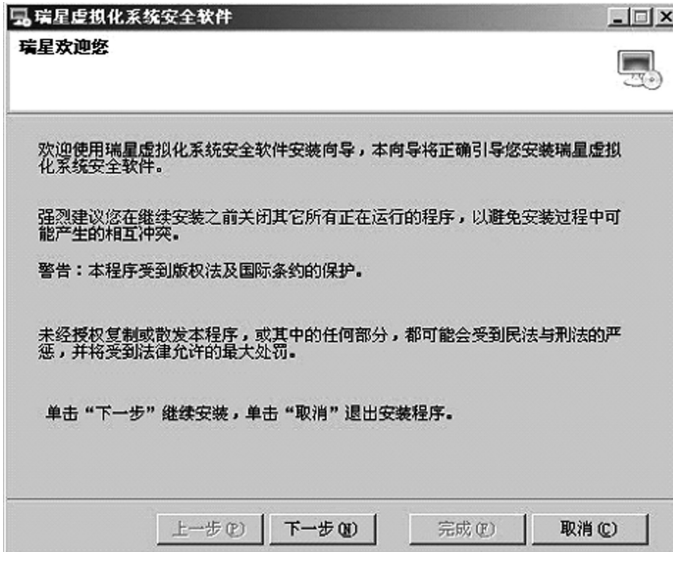
3.2 组件安装

3.2.1 管理中心

第一步：将瑞星虚拟化系统安全软件光盘放入光驱内，启动产品安装主界面后，开始安装。

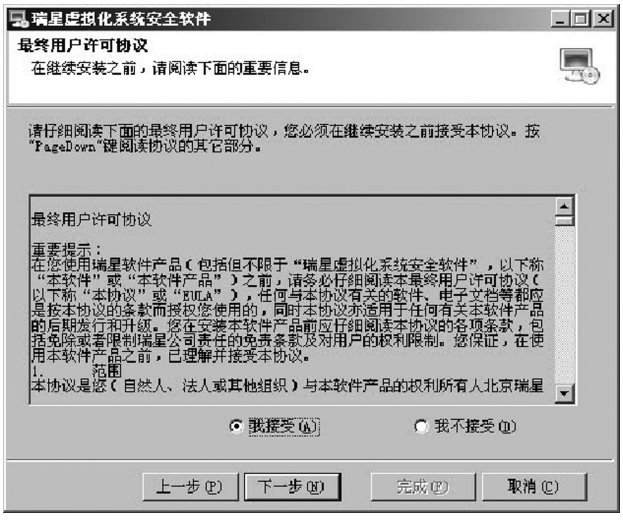
图表 3-2

第二步：进入安装程序欢迎界面，提示用户使用安装向导以及相关建议和警告等，点击【下一步】继续安装，或点击【取消】退出安装过程。



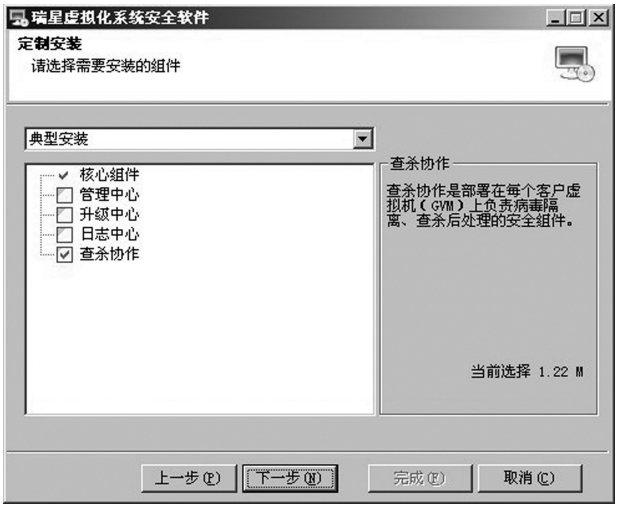
图表 3-3

第三步：提示用户在安装前阅读【最终用户许可协议】，用户认真阅读本协议后可以选择【我接受】或【我不接受】。选择【我接受】，点击【下一步】继续安装；选择【我不接受】，安装终止；点击【取消】直接退出安装过程。



图表 3-4

第四步：在【定制安装】界面选择【管理中心】组件，点击【下一步】继续安装。



图表 3-5

第五步：进入【数据库选项】界面，选择数据库的类型及相关参数（默认选中 MySQL 数据库）。设置 MySQL 数据库各项参数。

图表 3-6

提示：【数据库名称】填写可用数据库实例名称，如果没有数据库实例，需要进入 MySQL 管理控制台创建。具体操作方法请参考本文档章节 3.1.4 数据库。

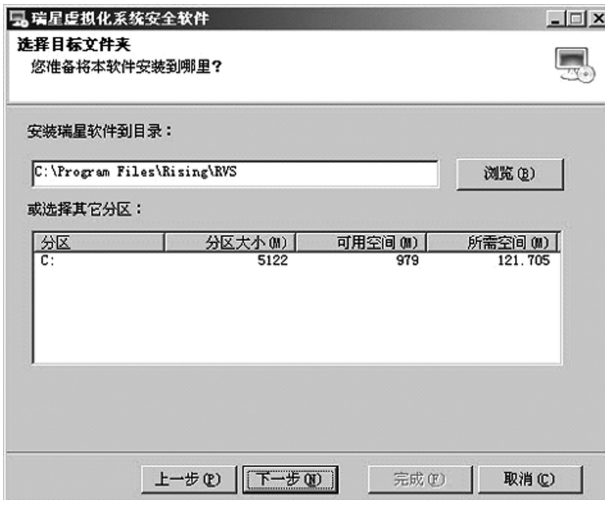
第六步：点击【测试连接】，提示“连接数据库成功”后点确定，点击【下一步】继续安装。

图表 3-7

第七步：在【管理中心选项】界面设定管理中心参数，点击【下一步】继续安装。

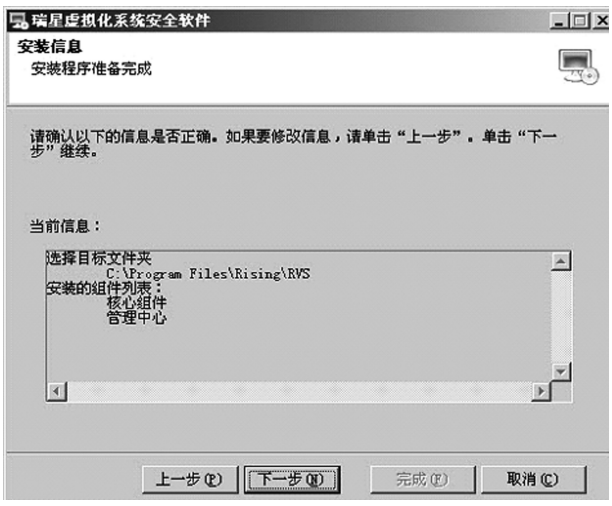
图表 3-8

第八步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。



图表 3-9

第九步：在【安装信息】界面中确认安装信息，点击【上一步】可进行修改，点击【下一步】继续安装。



图表 3-10

第十步：显示安装过程信息。

图表 3-11

第十一步：完成瑞星虚拟化系统安全软件管理中心安装过程。

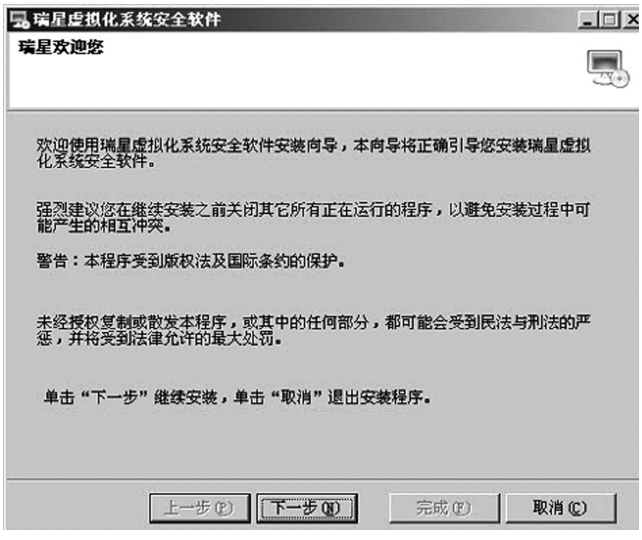
图表 3-12

3.2.2 日志中心

第一步：将瑞星虚拟化系统安全软件光盘放入光驱内，启动产品安装主界面后，开始安装。

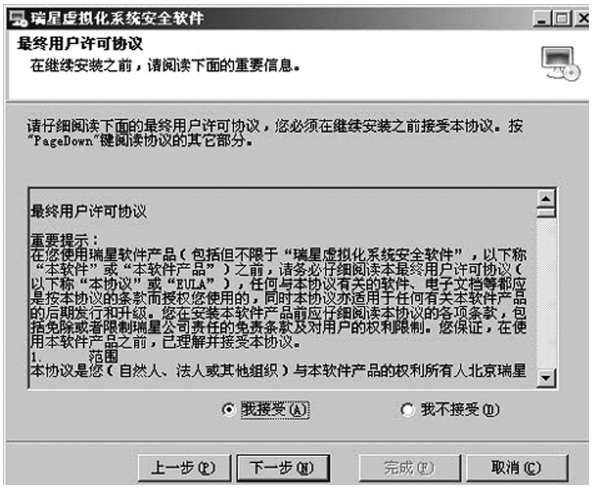
图表 3-13

第二步：进入安装程序欢迎界面，提示用户使用安装向导以及相关建议和警告等，点击【下一步】继续安装，或点击【取消】退出安装过程。



图表 3-14

第三步：提示用户在安装前阅读【最终用户许可协议】，用户认真阅读本协议后可以选择【我接受】或【我不接受】。选择【我接受】，点击【下一步】继续安装；选择【我不接受】，安装终止；点击【取消】直接退出安装过程。



图表 3-15

第四步：在【定制安装】界面选择【日志中心】组件，点击【下一步】继续安装。

图表 3-16

第五步：在【客户端选项】界面设定客户端参数，点击【下一步】继续安装。

图表 3-17

第六步：在【日志中心选项】界面设定日志中心参数，并配置数据库信息。

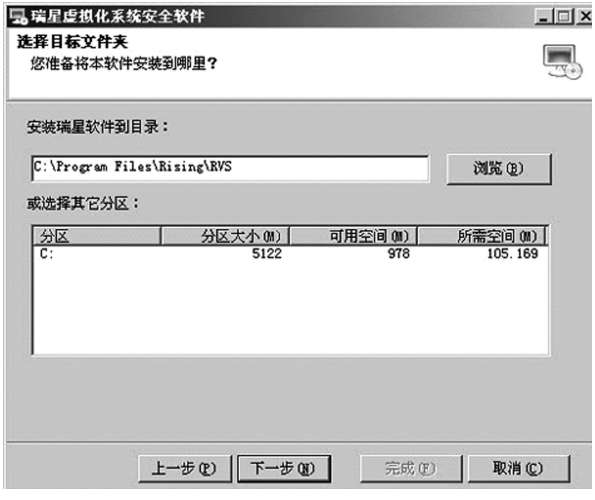
图表 3-18

提示：数据库配置需与管理中心保持一致。

第七步：点击【测试】，提示“连接数据库成功”后点确定，点击【下一步】继续安装。

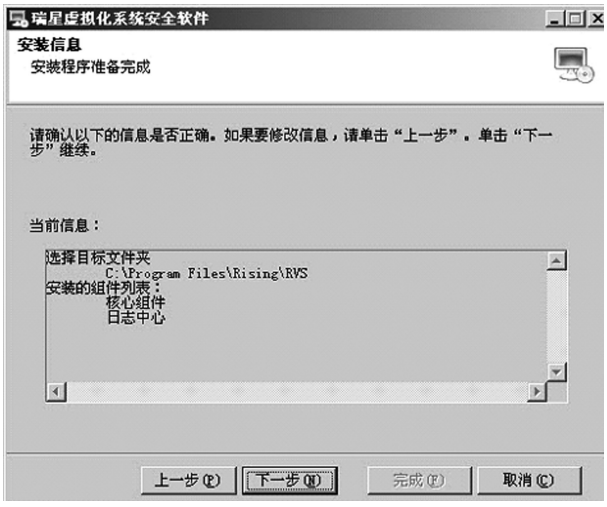
图表 3-19

第八步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。



图表 3-20

第九步：在【安装信息】界面中确认安装信息，点击【上一步】可进行修改，点击【下一步】继续安装。



图表 3-21

第十步：显示安装过程信息。

图表 3-22

第十一步：完成瑞星虚拟化系统安全软件日志中心安装过程。

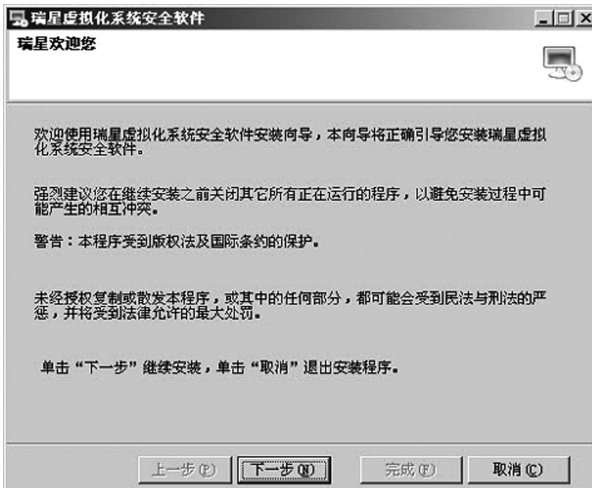
图表 3-23

3.2.3 升级中心

第一步：将瑞星虚拟化系统安全软件光盘放入光驱内，启动产品安装主界面后，开始安装。

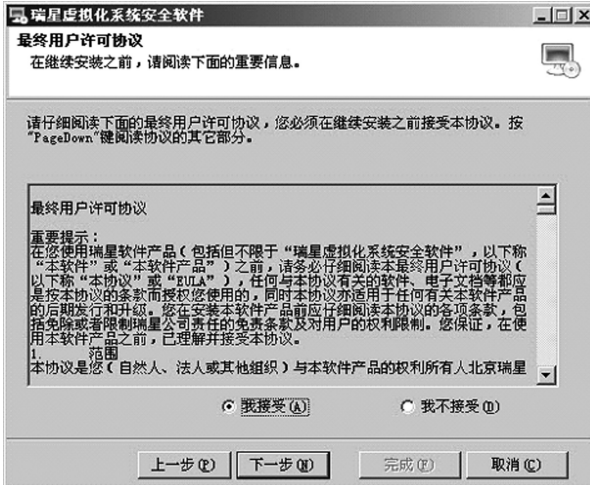
图表 3-24

第二步：进入安装程序欢迎界面，提示用户使用安装向导以及相关建议和警告等，点击【下一步】继续安装，或点击【取消】退出安装过程。



图表 3-25

第三步：提示用户在安装前阅读【最终用户许可协议】，用户认真阅读本协议后可以选择【我接受】或【我不接受】。选择【我接受】，点击【下一步】继续安装；选择【我不接受】，安装终止；点击【取消】直接退出安装过程。



图表 3-26

第四步：在【定制安装】界面选择【升级中心】组件，点击【下一步】继续安装。

图表 3-27

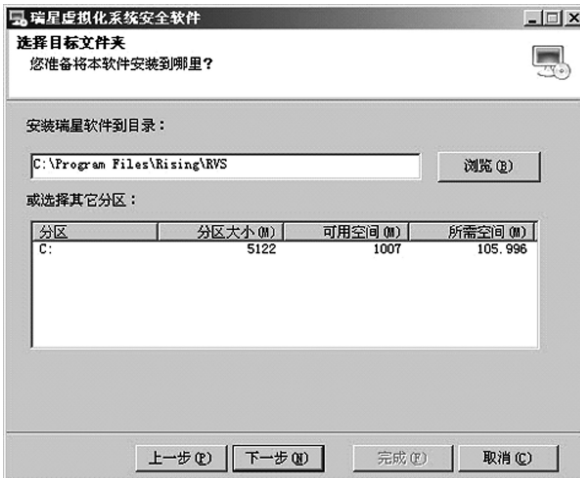
第五步：在【客户端选项】界面设定客户端参数，点击【下一步】继续安装。

图表 3-28

第六步：在【升级中心选项】界面设定升级中心参数，点击【下一步】继续安装。

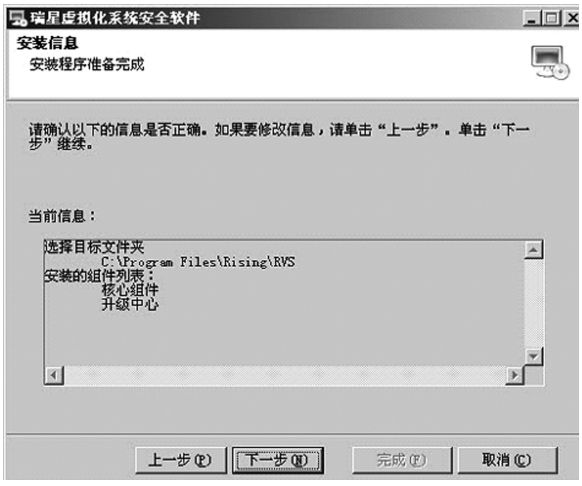
图表 3-29

第七步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。



图表 3-30

第八步：在【安装信息】界面中确认安装信息，点击【上一步】可进行修改，点击【下一步】继续安装。



图表 3-31

第九步：显示安装过程信息。

图表 3-32

第十步：完成瑞星虚拟化系统安全软件升级中心安装过程。

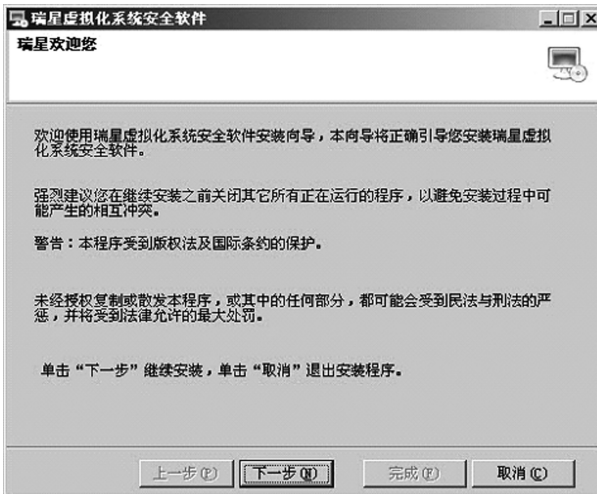
图表 3-33

3.2.4 查杀协作

第一步：将瑞星虚拟化系统安全软件光盘放入光驱内，启动产品安装主界面后，开始安装。

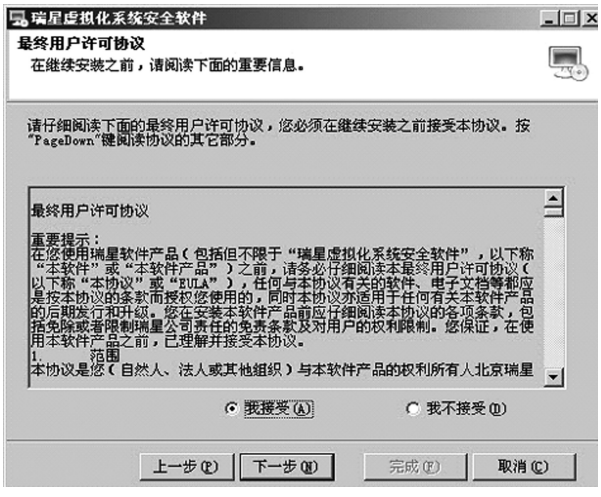
图表 3-34

第二步：进入安装程序欢迎界面，提示用户使用安装向导以及相关建议和警告等，点击【下一步】继续安装，或点击【取消】退出安装过程。



图表 3-35

第三步：提示用户在安装前阅读【最终用户许可协议】，用户认真阅读本协议后可以选择【我接受】或【我不接受】。选择【我接受】，点击【下一步】继续安装；选择【我不接受】，安装终止；点击【取消】直接退出安装过程。



图表 3-36

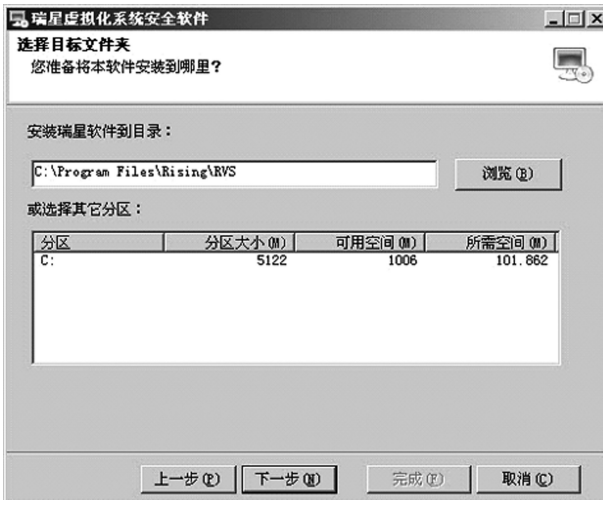
第四步：在【定制安装】界面选择【查杀协作】组件，点击【下一步】继续安装。

图表 3-37

第五步：在【客户端选项】界面设定客户端参数，点击【下一步】继续安装。

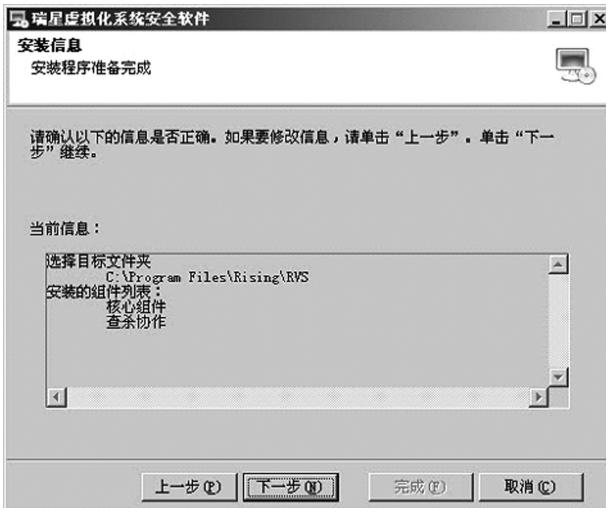
图表 3-38

第六步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。



图表 3-39

第七步：在【安装信息】界面中确认安装信息，点击【上一步】可进行修改，点击【下一步】继续安装。



图表 3-40

第八步：显示安装过程信息。

图表 3-41

第九步：完成瑞星虚拟化系统安全软件查杀协作安装过程。

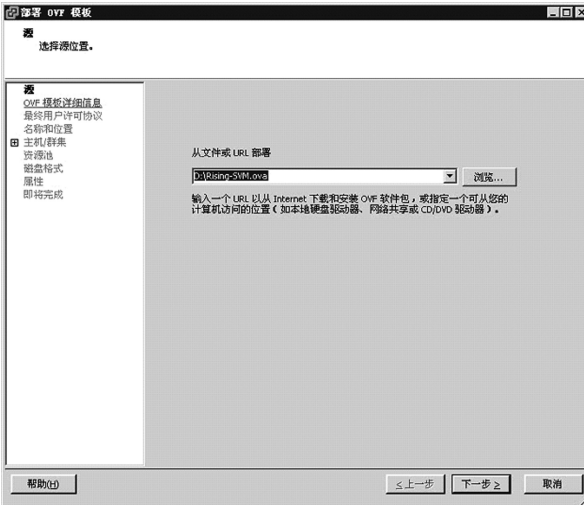
图表 3-42

3.2.5 安全虚拟设备

第一步：在 vSphere Client 界面中点击【文件】，选择【部署 OVF 模板】。

图表 3-43

第二步：在【源】界面选择安全虚拟设备模板文件源位置，点击【下一步】继续部署。



图表 3-44

第三步：在【OVF 模板详细信息】界面显示验证 OVF 模板详细信息，点击【下一步】继续部署。

图表 3-45

第四步：在【最终用户许可协议】界面，阅读协议文本，选择【接受】，点击【下一步】继续安装；或点击【取消】直接退出部署过程。

图表 3-46

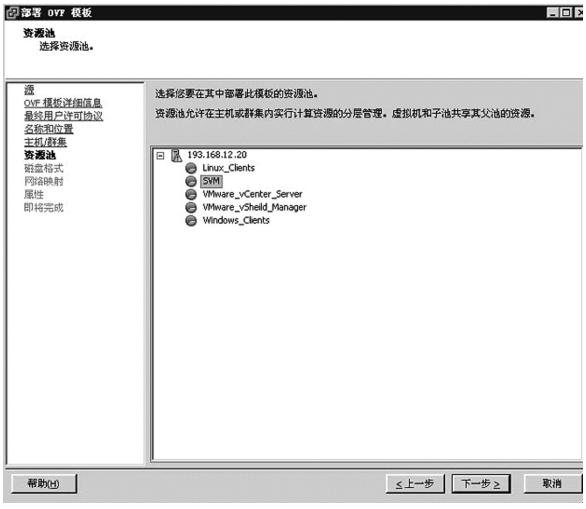
第五步：在【名称和位置】界面为安全虚拟设备指定名称和组位置，点击【下一步】继续部署。

图表 3-47

第六步：在【主机 / 群集】界面选择部署安全虚拟设备模板的主机或群集，点击【下一步】继续部署。

图表 3-48

第七步：在【资源池】界面选择部署安全虚拟设备模板的资源池，点击【下一步】继续部署。



图表 3-49

第八步：在【磁盘格式】界面选择 Thin Provision 格式储存虚拟磁盘，点击【下一步】继续部署。

图表 3-50

第九步：在【网络映射】界面选择安全虚拟设备模板的网络映射，点击【下一步】继续部署。

图表 3-51

第十步：在【属性】界面定义安全虚拟设备的网络配置信息，包括主机名、管理中心入口、IP 地址等，点击【下一步】继续部署。

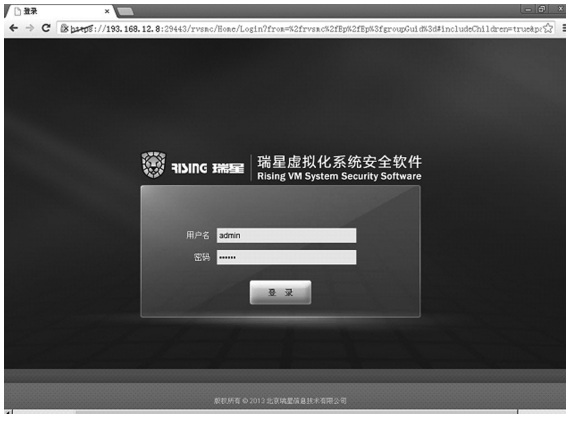
图表 3-52

第十一步：在【即将完成】界面中确认完整部署信息，点击【完成】，执行安全虚拟设备的部署。可以勾选【部署后打开电源】，安全虚拟设备部署完成后将处于启动状态。

图表 3-53

3.3 **导入** vCenter **终端**

第一步：在浏览器中打开瑞星虚拟化系统安全软件管理中心服务器地址，输入用户名、密码，进行登录。

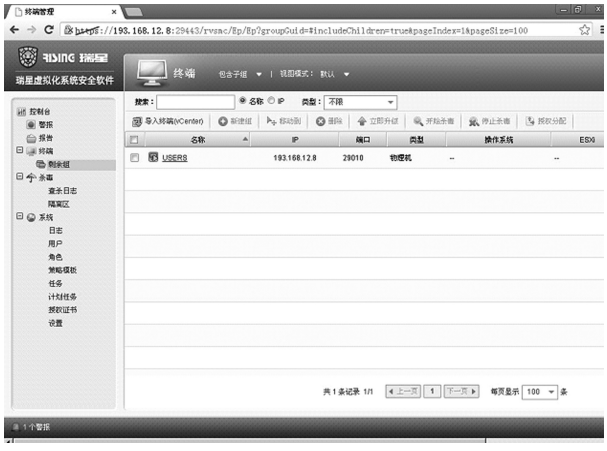


图表 3-54

第二步：显示瑞星虚拟化系统安全软件管理控制台主界面。

图表 3-55

第三步：点击控制台导航窗口的【终端】，点击工具栏的【导入终端（vCenter）】。

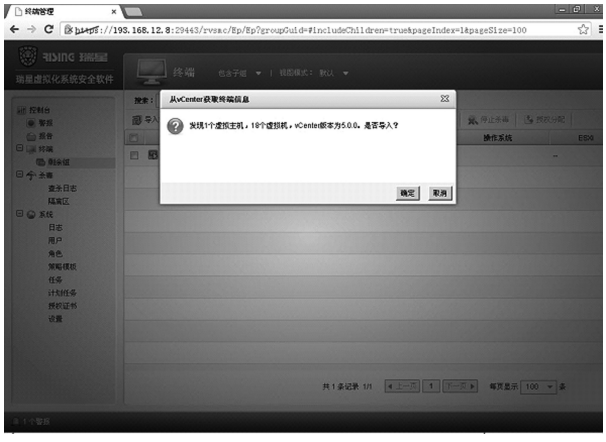


图表 3-56

第四步：在【从 vCenter 获取终端信息】页面中，填写 vCenter 管理中心信息、填写 vShield 管理中心信息，点击【下一步】。

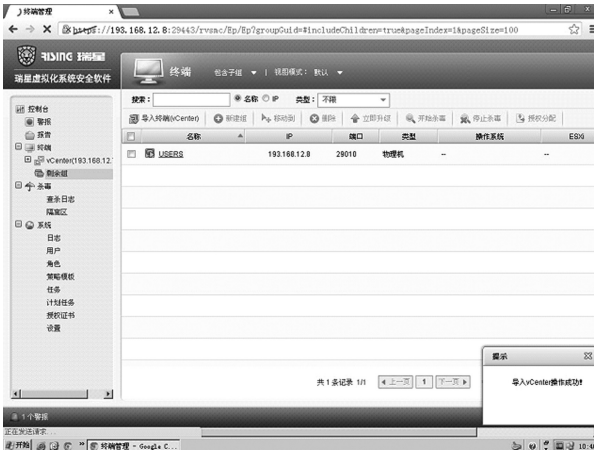
图表 3-57

第五步：在【从 vCenter 获取终端信息】页面中显示发现的虚拟主机数、虚拟机数和 vCenter 版本信息，点击【确定】导入瑞星虚拟化系统安全软件控制台。



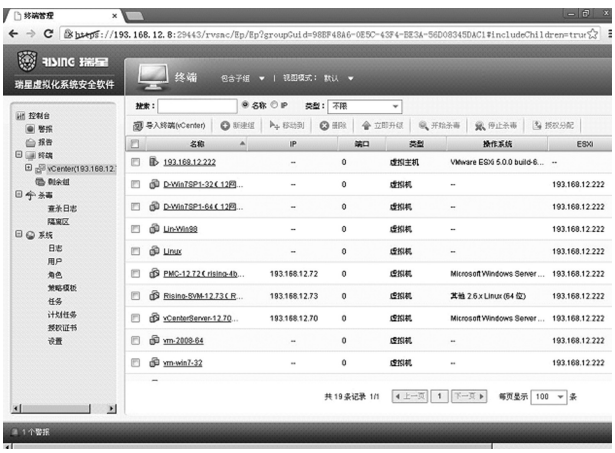
图表 3-58

第六步：确定导入后，右下角弹出窗口提示：导入 vCenter 操作成功。



图表 3-59

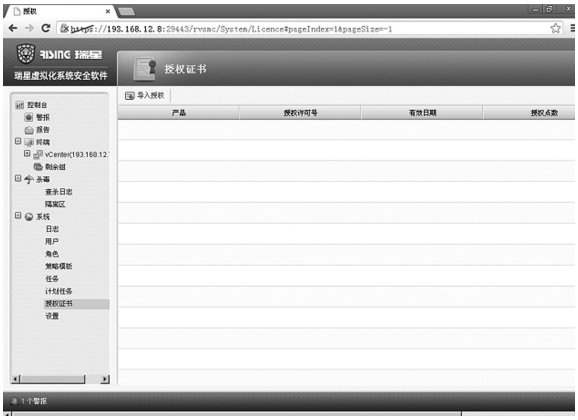
第七步：点击瑞星虚拟化系统安全软件控制台目录下的【终端】/【vCenter】，显示虚拟主机及所有虚拟机的详细信息。



图表 3-60

3.4 导入授权证书

第一步：点击控制台目录下的【系统】/【授权证书】，显示授权证书页面。



图表 3-61

第二步：点击【导入授权】，输入基本号、选择文件证书导入后【确定】。

图表 3-62

第三步：确定导入授权后，在【授权证书】页面显示授权许可的详细信息。

图表 3-63

3.5 激活安全虚拟设备

第一步：点击控制台导航窗口的【终端】/【vCenter 终端】，显示终端设备。

图表 3-64

第二步：点击安全虚拟设备，显示其激活状态。

图表 3-65

第三步：点击【激活】按钮，确定激活安全虚拟设备。

图表 3-66

第四步：激活完成后，右下角弹出窗口提示：激活成功。

图表 3-67

3.6 分配产品授权

3.6.1 单独分配

第一步：点击控制台导航窗口的【终端】/【vCenter 终端】，在终端窗口中点击安全虚拟设备，显示其授权状态。

图表 3-68

提示：只能为开启状态的安全虚拟设备分配授权。

第二步：选择杀毒【已授权】，点击【确定】按钮，分配杀毒产品授权。

图表 3-69

提示：安全虚拟设备占用的授权计数为其所属物理主机的 CPU 个数。

第三步：授权分配完成后，右下角弹出窗口提示：授权设置成功。

图表 3-70

提示：重复上述步骤可以为多个安全虚拟设备分配产品授权，但授权计数之和不能超过授权证书许可的点数。

3.6.2 批量分配

第一步：点击控制台导航窗口的【终端】/【vCenter 终端】，在终端窗口中勾选一个或多个安全虚拟设备。

图表 3-71

第二步：点击工具栏【授权分配】按钮，显示授权分配窗口。

图表 3-72

第三步：为安全虚拟设备勾选【授权分配】，点击【完成】，分配杀毒产品授权。

图表 3-73

第四步：授权分配完成后，右下角弹出窗口提示：所选终端分配授权成功！。

图表 3-74

提示：多个安全虚拟设备的授权计数之和不能超过授权证书许可的点数。

3.7 组件卸载

3.7.1 安全虚拟设备

第一步：点击控制台导航窗口的【终端】/【vCenter 终端】，在终端窗口中点击安全虚拟设备，显示其激活状态和授权状态。

图表 3-75

第二步：点击【撤销激活】按钮，确定撤销激活安全虚拟设备，右下角弹出窗口提示：撤销激活成功。

图表 3-76

第三步：选择杀毒【未授权】，点击【确定】按钮，右下角弹出窗口提示：授权设置成功。

图表 3-77

提示：只能为开启状态的安全虚拟设备撤销授权。

第四步：在 vSphere Client 界面左侧终端结构中选中待卸载的安全虚拟设备，点击右键，弹出快捷菜单。选择【从磁盘删除】，在弹出的删除确认窗口点击【是】，完成删除安全虚拟设备。

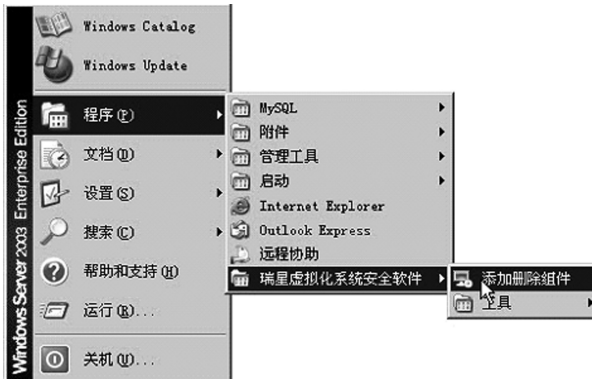
图表 3-78

第五步：点击管理控制台目录下的 vCenter，点击右上角【刷新 vCenter】，终端列表中不再出现待卸载的安全虚拟设备。

图表 3-79

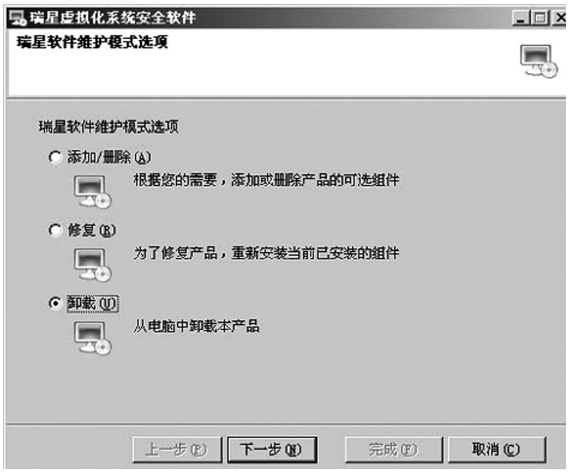
3.7.2 其他组件

第一步：在 Windows 画面中，选择【开始】/【程序】/【瑞星虚拟化系统安全软件】/【添加删除组件】。



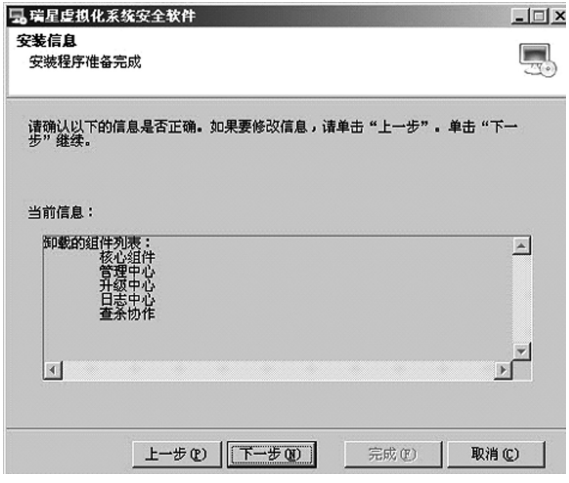
图表 3-80

第二步：在弹出的【瑞星软件维护模式选项】界面中选择【卸载】，点击【下一步】开始卸载。



图表 3-81

第三步：确认卸载信息，点击【上一步】可进行修改，点击【下一步】继续。



图表 3-82

第四步：显示卸载进度信息。

图表 3-83

第五步：点击【完成】，卸载结束。

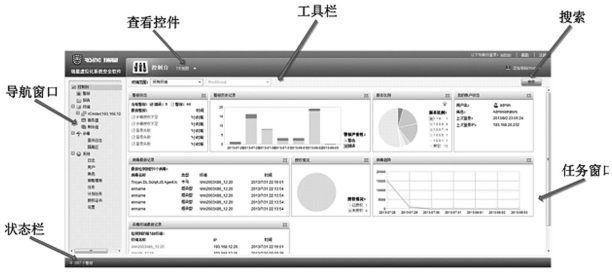
图表 3-84

第四章 系统管理

系统管理功能使得管理员能够对虚拟机网络中的全部终端进行统一配置、管理以及安全状况监测，从而保障整个虚拟机网络的安全。

4.1 管理中心

管理中心提供的管理控制台是瑞星虚拟化系统安全软件集中管理所有客户虚拟机安全状态的管理工具。管理员通过管理控制台，可以了解整个虚拟机网络的总体安全状况，直观的查看所有客户虚拟机当前的实时监控状态、病毒查杀情况、组件版本信息等；能够对任意客户虚拟机执行远程安全管理，进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个虚拟机网络中建立起坚实的安全防护系统。



图表 4-1

导航窗口：导航窗口包含树状结构的功能导航系统。

任务窗口：点击导航窗口中的功能节点，任务窗口中即会显示该功能的界面，几乎所有操作都能够在任务窗口中完成。

查看控件：任务窗口显示的内容可能包含很多项目，无法全部显示。在这种情况下，使用查看控件的筛选条件，可以切换任务窗口显示内容的子集。

工具栏：工具栏包含可对所在的任务窗口执行各种相应操作的按钮，通常包括删除、修改及创建项目列表的按钮。

搜索：可以选择终端范围、设定组及其他搜索条件进行搜索。

状态栏：状态栏会显示虚拟化系统当前状态的相关信息。状态栏左侧会显示活动警报的数量（如果有）。

4.1.1 控制台

4.1.1.1 时间视图

控制台显示过去 24 小时或过去七天的数据。可以使用窗口顶部的下拉菜单，切换时间视图。

图表 4-2

4.1.1.2 Widget

控制台信息通过信息面板 Widget 进行展示。Widget 支持拖放到新位置，以对其进行重新排列。也可以在管理控制台首页上添加或移除 Widget，方法为点击管理控制台右上方的【添加 / 移除 Widget】，勾选或取消勾选 Widget。

图表 4-3

4.1.1.3 搜索

控制台信息支持条件搜索，可选条件包括：组、子组和终端名称 /IP。

图表 4-4

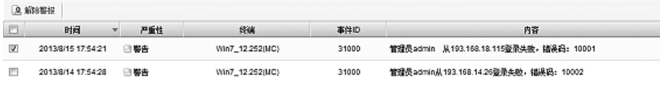
4.1.2 警报

警报窗口显示所有活动的警报，警报信息包括时间、严重性、终端、事件 ID 以及内容。

警报信息支持条件搜索，可选条件包括：组、子组、终端名称、事件 ID 以及时间范围。

图表 4-5

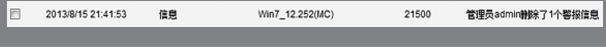
勾选警报记录，点击 解除警报 ，可以删除该警报记录



时间	严重性	终端	事件ID	内容
2013/8/15 17:54:21	警告	Win7_12.252(MC)	31000	管理员admin 从193.168.18.115登录失败，错误码：10001
2013/8/14 17:54:28	警告	Win7_12.252(MC)	31000	管理员admin从193.168.14.26登录失败，错误码：10002

图表 4-6

提示：【系统】-【日志】中将自动记录删除警报记录的活动信息。

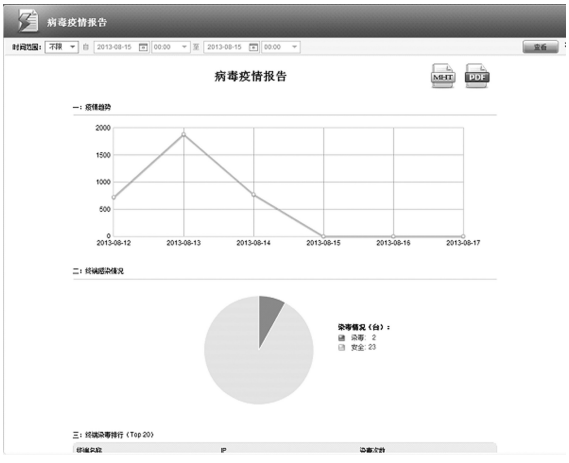


	2013/8/15 21:41:53	信息	Win7_12.252(MC)	21500	管理员admin删除了1个警报信息

4.1.3 报告

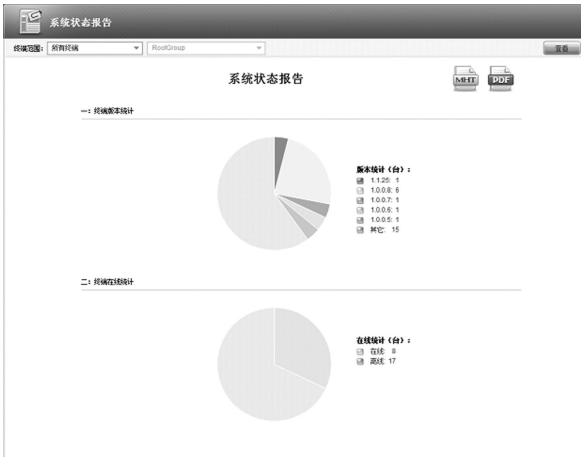
报告分为【病毒疫情报告】和【系统状态报告】两类。

【病毒疫情报告】主要提供详尽的病毒趋势、终端染毒情况、病毒类型的分析报告，支持根据筛选条件进行报告的查看及导出，筛选条件包括组、子组、终端名称 /IP 以及时间范围，导出格式包括 MHT 和 PDF。



图表 4-7

【系统状态报告】主要提供详尽的终端在线情况以及升级情况，支持根据筛选条件进行报告的查看及导出，筛选条件包括组、子组、终端名称 /IP，导出格式包括 MHT 和 PDF。



图表 4-8

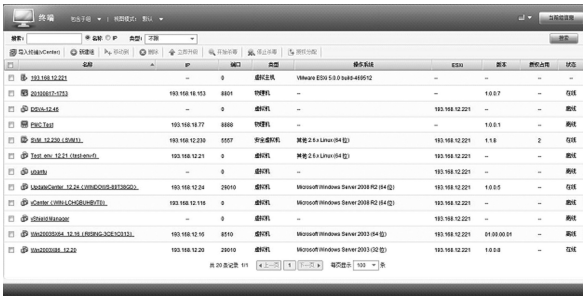
4.1.4 **终端**

终端窗口显示可以监控和管理的网络上的终端组织结构信息，包括名称、IP、端口、类型、操作系统、ESXi、版本、授权占用和状态。

终端窗口支持条件搜索，可选条件包括：终端名称 /IP、类型（包括不限、虚拟主机、安全虚拟设备、虚拟机、物理机）。

图表 4-9

终端窗口会定期自动更新，点击表头，可以按照相应字段排序。



图表 4-10

4.1.4.1 组

导航窗口显示的终端组分为三类，包括 vCenter 导入组、自定义组、剩余组 。其中：

4.1.4.1.1 vCenter 导入组

vCenter 导入组信息从 vCenter 获取，内部结构只读。点击右上角操作当前组图表，可以对 vCenter 导入组执行刷新、删除、立即升级、开始杀毒、停止杀毒操作。

图表 4-11

vCenter 导入组内终端类型为虚拟机，选中组内的终端，可以点击工具栏中 立即升级 、开始杀毒 、停止杀毒 进行终端组件的升级、启动杀毒、终止杀毒操作。

选中 vCenter 导入组，点击右上角 当前组信息 ，显示其详细信息，包括组信息、警报记录、杀毒策略、查杀日志记录、隔离区记录、日志记录、任务状态以及升级策略信息。

组信息

【组信息】显示基本信息和 vCenter & vShield 信息。修改信息后，点击 保存 生效。

图表 4-12

警报

【警报】显示组相关警报记录，具体操作方法请参考本文档章节 4.1.2 警报。

杀毒

【杀毒】显示组相关扫描、文件监控和隔离区策略信息。

扫描策略和文件监控策略具体操作方法请分别参考本文档章节 4.1.6.4 策略模板扫描策略和文件监控策略部分。隔离区策略显示隔离区空间不足时处理方式和隔离区大小设置，勾选【隔离区使用默认策略】，设置使用产品默认策略。

图表 4-13

查杀日志

【查杀日志】显示组相关查杀日志记录，具体操作方法请参考本文档章节 4.1.5.1 查杀日志。

隔离区

【隔离区】显示组相关隔离区记录，具体操作方法请参考本文档章节 4.1.5.2 隔离区。

日志

【日志】显示组相关日志记录，具体操作方法请参考本文档章节 4.1.6.1 日志。

任务

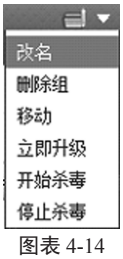
【任务】显示组相关任务状态，具体操作方法请参考本文档章节 4.1.6.5 任务。

升级

【升级】显示组升级和日志策略信息，勾选【使用默认策略】，设置使用产品默认策略；不勾选【使用默认策略】，可以单独设置策略，具体操作方法请参考本文档章节 4.1.6.4 策略模板。

4.1.4.1.2 自定义组

自定义组是用户自行建立的组，可以点击工具栏中的 新建组 在组内创建自定义组，点击右上角操作当前组图表，可以对自定义组执行改名、删除、移动、立即升级、开始杀毒、停止杀毒操作。



图表 4-14

自定义组内终端类型为物理机，选中组内的终端，可以点击工具栏中的 移动到 、 删除 进行终端的移动和删除操作，点击 立即升级 进行终端组件的升级。

选中自定义组，点击右上角 当前组信息 ，显示其详细信息，包括组信息、警报记录、日志记录、任务状态以及升级策略信息，具体操作方法请参考本文档章节 4.1.4.1.1vCenter 导入组。

4.1.4.1.3 剩余组

剩余组是系统预留的组，组内终端类型为物理机，安装查杀协作组件后的物理机将被自动发现并加入剩余组中。

剩余组内终端类型为物理机，选中组内的终端，可以点击工具栏中的 移动到 、 删除 进行终端的移动和删除操作，点击 立即升级 进行终端组件的升级。

4.1.4.2 虚拟主机

点击虚拟主机名称，显示其详细信息，包括终端信息、警报记录、日志记录以及任务状态信息。

终端信息

【终端信息】显示虚拟主机名称、类型、所属组、IP 地址、端口、操作系统、版本及备注信息。可以修改备注信息，点击 保存 生效。

图表 4-15

警报

【警报】显示虚拟主机相关警报记录，具体操作方法请参考本文档章节 4.1.2 警报。

日志

【日志】显示虚拟主机相关日志记录，具体操作方法请参考本文档章节 4.1.6.1 日志。

任务

【任务】显示虚拟主机相关任务状态，具体操作方法请参考本文档章节 4.1.6.5 任务。

4.1.4.3 安全虚拟设备

点击安全虚拟设备名称，显示其详细信息，包括终端信息、警报记录、病毒白名单、日志记录、任务状态以及升级策略信息。

终端信息

【终端信息】显示安全虚拟设备名称、类型、所属组、IP 地址、端口、操作系统、版本及备注信息。点击 立即升级 ，可以执行安全虚拟设备组件升级操作，还可以修改备注信息，点击 保存 生效。

【激活状态】显示安全虚拟设备激活状态，具体操作方法请参考本文档章节 3.5 激活安全虚拟设备第二步至第四步和 3.7.1 安全虚拟设备第二步。

【授权状态】显示安全虚拟设备授权状态，具体操作方法请参考本文档章节 3.6.1 单独分配第二步至第三步和 3.7.1 安全虚拟设备第三步。

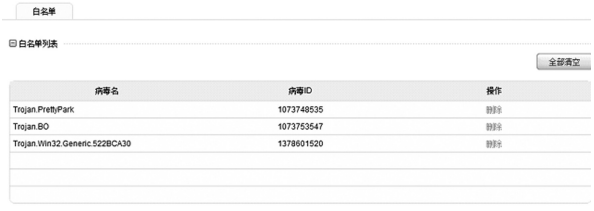
图表 4-16

警报

【警报】显示安全虚拟设备相关警报记录，具体操作方法请参考本文档章节 4.1.2 警报。

病毒白名单

【病毒白名单】显示自客户虚拟机隔离区手工恢复的病毒记录，进入病毒白名单的病毒记录将不会被报毒。点击 删除 ，删除单条病毒记录，点击 全部清空 ，删除全部病毒记录。



图表 4-17

日志

【日志】显示安全虚拟设备相关日志记录，具体操作方法请参考本文档章节 4.1.6.1 日志。

任务

【任务】显示安全虚拟设备相关任务状态，具体操作方法请参考本文档章节 4.1.6.5 任务。

升级

【升级】显示安全虚拟设备升级和日志策略信息，勾选【继承组策略】，设置策略与父组一致；不勾选【继承组策略】，可以单独设置策略，具体操作方法请参考本文档章节 4.1.6.4 策略模板。

图表 4-18

4.1.4.4 虚拟机

点击虚拟机名称，显示其详细信息，包括终端信息、警报记录、杀毒策略、查杀日志、隔离区、日志记录、任务状态以及升级策略信息。

终端信息

【终端信息】显示虚拟机名称、类型、所属组、IP 地址、端口、操作系统、版本及备注信息。点击 立即升级 ，可以执行虚拟机查杀协作组件升级操作，还可以修改备注信息，点击 保存 生效。

图表 4-19

警报

【警报】显示虚拟机相关警报记录，具体操作方法请参考本文档章节 4.1.2 警报。

杀毒

【杀毒】显示虚拟机相关扫描、文件监控和隔离区策略信息，具体操作方法请参考本文档章节 4.1.4.1.1vCenter 导入组杀毒部分。

日志

任务

升级

【日志】、【任务】、【升级】显示虚拟机相关日志记录、任务状态、升级和日志策略信息，具体操作方法请参考本文档章节 4.1.4.3 安全虚拟设备日志、任务、升级部分。

4.1.4.5 物理机

点击物理机名称，显示其详细信息，包括终端信息、警报记录、日志记录、任务状态以及升级策略信息，具体操作方法请参考本文档章节 4.1.4.4 虚拟机终端信息、警报、日志、任务、升级部分。

4.1.5 **杀毒**

杀毒功能针对基于文件的威胁（包括常称为恶意软件、病毒、特洛伊木马以及间谍软件的威胁）同时提供实时保护和按需保护。为识别威胁，杀毒功能会使用病毒库对文件进行检查，该病毒库文件存放在安全虚拟设备上。

4.1.5.1 杀毒策略

点击【杀毒】，管理杀毒策略，具体操作方法请参考本文档章节 4.1.6.4 策略模板。

4.1.5.2 查杀日志

管理中心实时收集查杀结果，记录查杀日志，供管理员查询以及生成各种图表、报告使用。

查杀日志信息包括查杀时间、终端名称、终端 IP、发现病毒名称、病毒类型（划分为未知、蠕虫、后门、木马、感染型、垃圾邮件、恶意程序、黑客工具、其他）、染毒文件全路径名称以及处理结果。

处理结果

【清除成功】已成功终止恶意软件进程并删除病毒造成的文件、注册表、cookie 或快捷方式修改。

【清除失败】因各种可能的原因而无法清除病毒。

【删除成功】已删除受病毒感染的文件。

【删除失败】因各种可能的原因而无法删除受病毒感染文件。例如，文件可能由其他应用程序锁定、文件位于 CD 上或者正在使用中，如果可能，将在受病毒感染文件被释放后立即将其删除。

【查杀失败】因各种原因可能导致查杀失败。

【已忽略】未采取任何处理措施，但记录了对病毒的检测。

查杀日志支持条件搜索，可选条件包括：终端范围、组、病毒类型、处理结果、病毒名称以及时间范围。

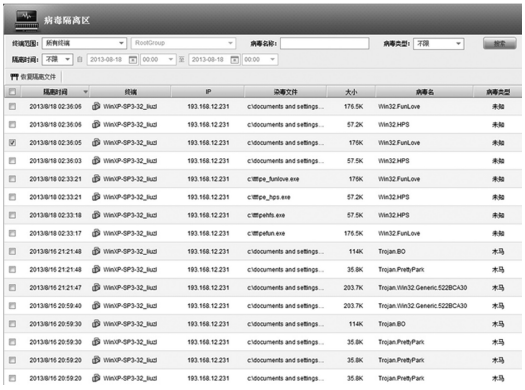
图表 4-20

4.1.5.3 隔离区

隔离的文件是已查明为（或包含）病毒且因此已进行加密并移动到终端特殊文件夹中的文件。隔离区策略设置具体方法请参考本文档章节 4.1.4.1.1vCenter 导入组杀毒部分。

隔离区文件信息包括隔离时间、终端名称、终端IP、文件全路径名称、文件大小、感染病毒名称以及病毒类型（划分为未知、蠕虫、后门、木马、感染型、垃圾邮件、恶意程序、黑客工具、其他）。

隔离区文件信息支持条件搜索，可选条件包括：终端范围、组、病毒名称、病毒类型以及隔离时间范围。



图表 4-21

勾选隔离区文件信息，点击 恢复隔离文件，可以将隔离文件恢复到终端上。

4.1.6 系统

4.1.6.1 日志

日志提供了审查瑞星系统安全软件运行事件记录的功能。日志策略设置具体操作方法请参考本文档章节 4.1.6.4 策略模板日志策略部分。

日志窗口显示所有日志记录，日志记录信息包括时间、严重性、终端、事件 ID 以及内容。

日志记录信息支持条件搜索，可选条件包括：终端范围、组、严重性、事件 ID 以及时间范围。

图表 4-22

4.1.6.2 用户

用户是指管理中心帐户持有者。

用户窗口显示所有用户帐户，用户帐户信息包括用户名、描述、角色名称、上次登录时间、上次登录 IP 以及状态。

图表 4-23

点击工具栏中的 新增 ，设置用户名、密码、备注、语言、角色和状态信息，可以创建新用户帐户。在用户窗口中点击用户名，可以对用户名和密码以外的信息进行修改。

图表 4-24

提示：角色信息请参考本文档章节 4.1.6.3 角色。

勾选用户信息，点击工具栏中的 删除、重置密码 可以进行用户帐户的删除和重置密码操作。

提示：admin 帐户无法删除

点击右上角登录用户名 以下列身份登录：admin ，可以快捷切换语言和修改密码。

4.1.6.3 角色

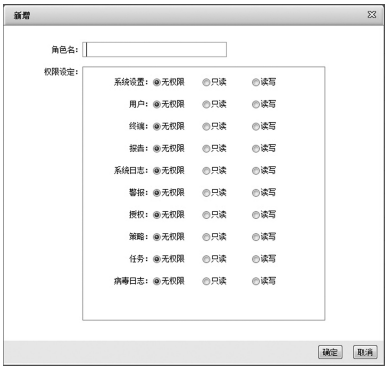
瑞星虚拟化系统安全软件使用基于角色的访问控制来限制用户对产品功能的使用。应为每个用户创建单独的帐户并分配角色，该角色将限制除那些完成其职责所必需的活动外的所有活动。

角色窗口显示所有角色，角色信息包括角色名和用户数。

管理中心随附了两个预先配置的角色：系统管理员（Administrators）和审计管理员。系统管理员角色授予用户有关管理瑞星虚拟化系统安全软件的所有可能权限（例如：创建、编辑和删除终端、组、策略等）；审计管理员为用户提供在瑞星虚拟化系统安全软件中查看所有信息的功能，但不能修改除其个人帐户信息之外的任何设置。

图表 4-25

点击工具栏中的 新增，可以设置角色名、选择权限设定、创建新角色。在角色窗口中点击角色名，可以对角色名和权限设定进行修改。



图表 4-26

勾选角色信息，点击工具栏中的 删除 ，可以进行角色的删除操作。

提示：系统管理员角色无法删除。

4.1.6.4 策略模板

瑞星虚拟化系统安全软件支持创建各种杀毒策略和终端代理策略模板，用于下发设置至组和终端，简化管理操作。

策略模板窗口显示所有策略模板，策略模板信息包括策略名称、子产品名称、分类、已分配组数量、已分配终端数量。

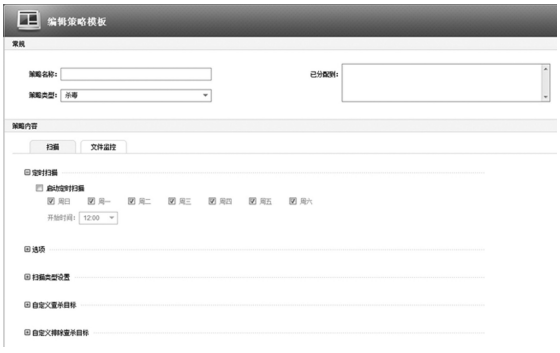
策略模板信息支持条件搜索，可选条件为产品。

图表 4-27

在策略模板窗口中勾选策略模板信息，点击工具栏中的 分配策略，可以选择策略模板分配到的组和终端。

图表 4-28

点击工具栏中的 新建策略模板 ，可以设置策略名称、策略类型和策略内容，建立新的策略模板。在策略模板窗口中点击策略模板名称，可以对策略模板信息进行修改。



图表 4-29

策略类型划分为杀毒和终端代理，其中，杀毒类型的策略内容包括扫描和文件监控，终端代理类型的策略内容包括升级和日志。

4.1.6.4.1 扫描策略

定时扫描

配置定时扫描的启用状态和开始时间。

图表 4-30

病毒处理选项

配置发现病毒时的处理方式、查杀文件大小限制、查杀压缩文件层数以及智能提速启用状态。

图表 4-31

扫描类型设置

配置安全级别，定义扫描文件类型和病毒类型。

图表 4-32

自定义查杀目标

配置扫描的文件扩展名和目录。

图表 4-33

自定义排除查杀目标

配置排除扫描的文件扩展名、目录和全路径。

图表 4-34

4.1.6.4.2 文件监控策略

文件监控选项

配置文件监控开启状态、发现病毒时的处理方式、查杀文件大小限制、查杀压缩文件层数以及智能提速启用状态。

图表 4-35

扫描类型设置

自定义查杀目标

自定义排除查杀目标

上述三项的具体操作方法请参考本文档章节 4.1.6.4.1 扫描策略扫描类型设置、自定义查杀目标、自定义排除查杀目标日志部分。

4.1.6.4.3 升级策略

定时设置

配置定时升级的启用状态和开始时间。

图表 4-36

升级方式设置

配置升级源地址。

图表 4-37

网络连接设置

配置网络连接方式。

图表 4-38

4.1.6.4.4 日志策略

日志中心

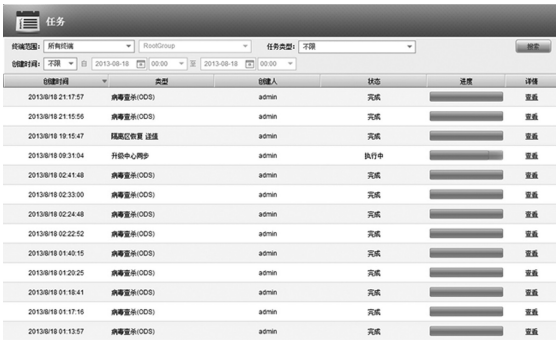
配置日志中心地址。

图表 4-39

4.1.6.5 任务

任务窗口显示所有任务事件，任务事件信息包括创建时间、类型、创建人、状态、进度以及详情链接。

任务事件信息支持条件搜索，可选条件包括：终端范围、组、任务类型以及创建时间范围。



图表 4-40

点击任务事件详情查看链接，显示任务完整信息。

图表 4-41

4.1.6.6 计划任务

计划任务支持自动化和预设某些常见任务，已设定的计划任务将根据预设的时间表启动。

计划任务窗口显示所有计划任务，计划任务信息包括名称、类型、创建人、时间计划以及状态。

图表 4-42

勾选计划任务细信息，点击工具栏中的 启用 、 禁用 、 删除 ，进行计划任务的启用、禁用和删除操作。

点击工具栏中的 新建计划任务，可以设置任务名称、类型（包括终端升级、病毒查杀（ODS）、升级中心同步）、时间计划以及执行目标，建立新的计划任务。在计划任务窗口中点击计划任务名称，可以对计划任务信息进行修改。

图表 4-43

4.1.6.7 授权证书

瑞星虚拟化系统安全软件采用证书机制进行子产品授权，每个子产品都可完全授权，或者授权使用试用版。

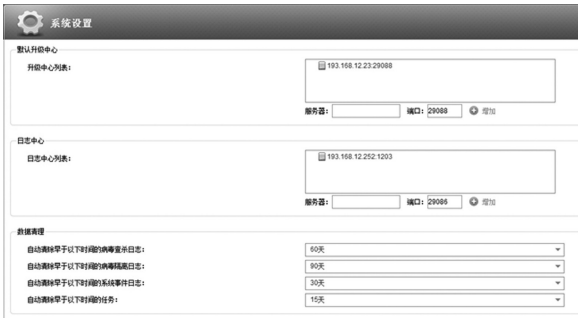
授权证书窗口显示有关瑞星虚拟化系统安全软件授权的详细信息，授权信息包括子产品、授权许可号、有效日期、授权点数以及状态。

图表 4-44

如果任意子产品将要过期或已过期，将会生成警报。如果需要升级使用授权，请与北京瑞星信息技术有限公司联系。获得新授权证书后的导入操作方法请参考本文档章节 3.4 导入授权证书。

4.1.6.8 设置

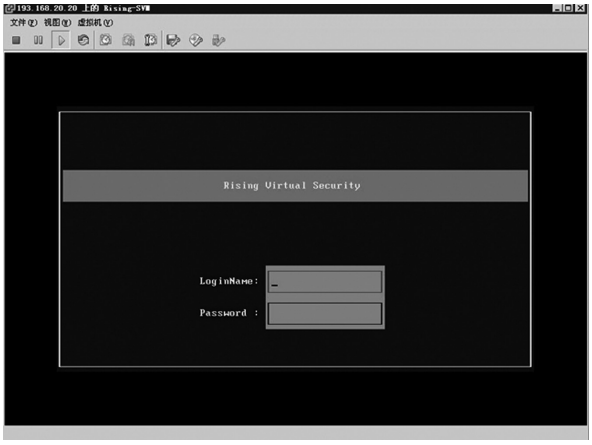
系统设置窗口提供对产品默认设置的管理，包括升级中心、日志中心和数据清理策略。



图表 4-45

4.2 安全虚拟设备

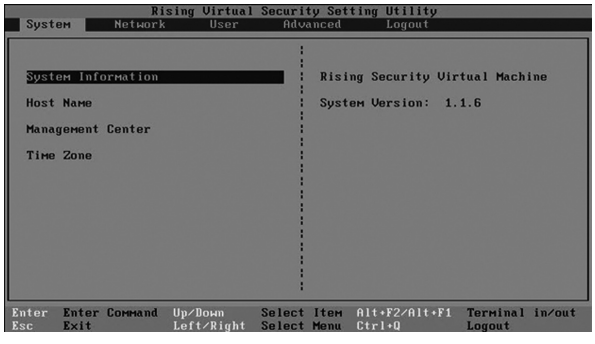
点击 VMware vSphere Client 中安全虚拟设备控制台选项卡，显示安全虚拟设备登录界面。



图表 4-46

4.2.1 系统信息

选中【System】页签，显示【System Information】安全虚拟设备版本号、【Host Name】主机名称、【Management Center】管理中心地址以及【Time Zone】时区配置信息。

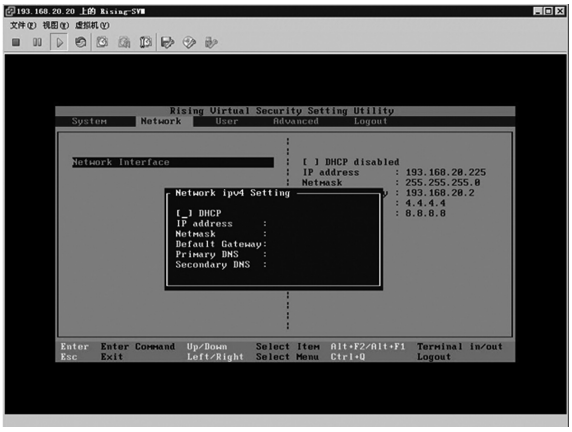


图表 4-47

4.2.2 配置管理网络

选中【Network】页签，显示【Network Interface】管理安全虚拟设备网络地址。

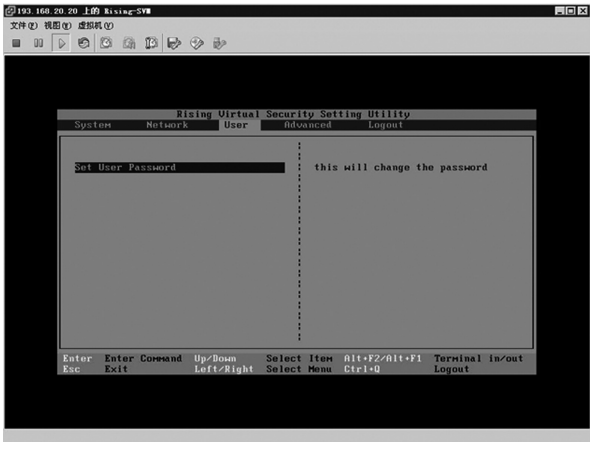
安全虚拟设备缺省使用本地 DHCP 服务器分配的 IP 地址。如果没有 DHCP 服务器，回车后手动输入 IP 地址信息。



图表 4-48

4.2.3 配置密码

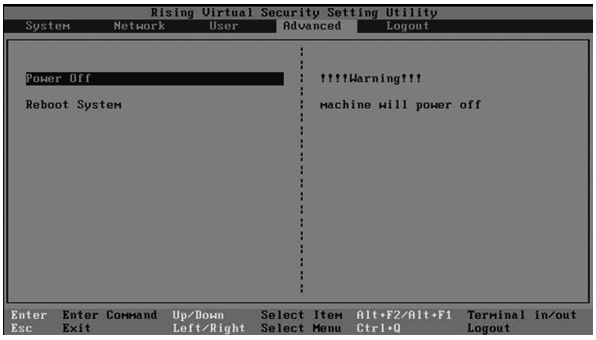
选中【USER】页签，显示【Set User Password】设置安全虚拟设备管理员密码。



图表 4-49

4.2.4 重启系统

选中【Advanced】页签，显示【Power Off】执行关闭或【Reboot System】重启安全虚拟设备的操作。关闭或重启前，将自动保存此前的配置信息。



图表 4-50

4.2.5 退出系统

选中【Logout】页签，显示【User Logout】退出安全虚拟设备登录界面。

图表 4-51

4.3 管理工具

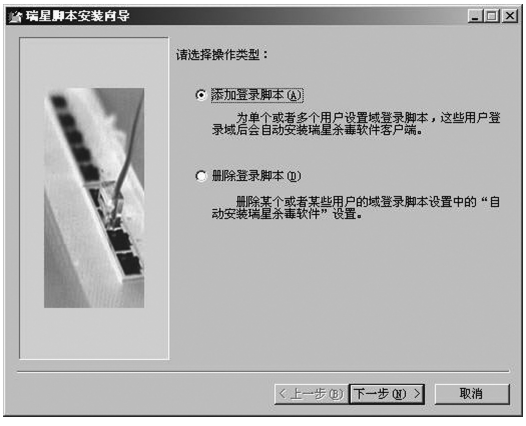
4.3.1 远程安装工具

瑞星虚拟化系统安全软件可通过管理员权限向所有网络邻居中的 Windows 2000/XP/2003/Vista/2008/2008 R2/7 服务器 / 工作站终端远程安装产品。

图表 4-52

4.3.2 域脚本安装工具

瑞星虚拟化系统安全软件利用域的启动服务概念，在域服务器上配置登录脚本，采用域策略下发的形式进行产品安装。当具有安装执行权限的用户登录到所在域时，登录终端将自动运行产品安装程序。

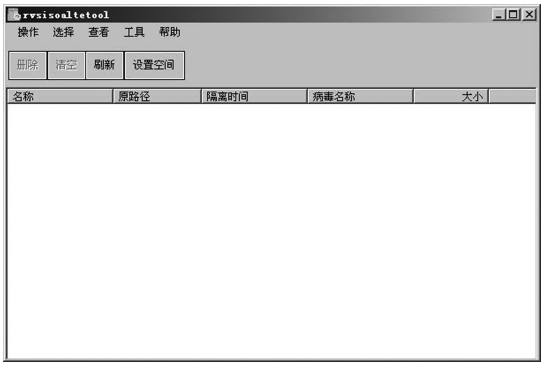


图表 4-53

4.3.3 隔离区管理工具

隔离区将染毒文件安全隔离并备份，用户可以从隔离区中对染毒文件进行恢复。此功能可防止用户误操作或异常情况下造成的文件损失，为用户提供一个统一的病毒文件恢复机制。

在终端 Windows 桌面，选择【开始】/【程序】/【瑞星虚拟化系统安全软件】/【病毒隔离区】，启动隔离区管理工具。



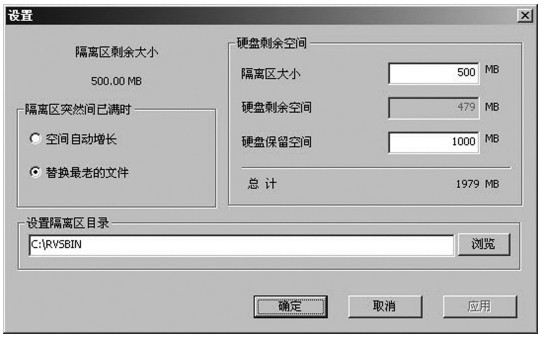
图表 4-54

【操作】 执行隔离区文件操作，包括恢复、恢复为、删除、清空以及关闭隔离区管理工具。

【选择】 执行隔离区文件选择，包括全部选定、反向选择、相同时间保存的文件、相同路径保存的文件以及被相同病毒感染的文件。

【查看】 执行查看，包括刷新列表、查看病毒资料和列项目。

【工具】 执行设置，包括设置隔离区空间、设置隔离区目录和设置硬盘保留空间。



图表 4-55

第五章 杀毒

5.1 手动查杀

操作步骤

- 启动并登录瑞星虚拟化系统安全软件管理中心控制台；
- 点击左侧导航窗口中的【终端】，显示所有被管理的终端；
- 勾选需要查杀的虚拟机终端，点击工具栏 开始杀毒 ；
- 查杀过程中，可以随时点击工具栏 停止杀毒，终止查杀病毒；
- 当查杀病毒时，点击【查杀日志】，实时查看查杀记录；
- 查杀结束后，全部查杀日志将自动保存，可以通过在查杀日志窗口中设定不同的搜索条件来查询特定的信息。

查杀策略设置请参考本文档章节 4.1.6.4.1 扫描策略。

5.2 文件监控

文件监控用于实时的监控虚拟化系统中的文件操作，在终端进行文件操作之前对文件查毒，从而阻止病毒运行，保护虚拟化系统安全。

文件监控发现病毒时，在管理中心控制台的查杀日志窗口会列出相应的病毒查杀记录信息。

监控策略设置请参考本文档章节 4.1.6.4.2 文件监控策略。

附录一 北京瑞星信息技术有限公司简介

瑞星品牌诞生于 1991 年刚刚在经济改革中蹒跚起步的中关村，是中国最早的计算机反病毒标志。在公安部组织的计算机病毒防治产品评测中，“瑞星杀毒软件”单机版和网络版连续多年蝉联第一的殊荣。

瑞星以研究、开发、生产及销售计算机反病毒产品、网络安全产品和反“黑客”防治产品为主，拥有全部自主知识产权和多项专利技术。几经重组，公司已形成一支中国最大的反病毒队伍。

目前，公司已推出基于多种操作系统的瑞星杀毒软件单机版、网络版客户端软件产品以及企业防毒墙、防火墙、网络安全预警系统等硬件产品，是全球第三家、也是国内唯一一家可以提供全系列信息安全产品和服务的专业厂商。

公司拥有国内最大、最具实力的反病毒和网络安全研发队伍，并且拥有国内安全行业唯一的“电信级”呼叫服务中心和“在线专家门诊”Online 服务系统。

瑞星和政府机构、商业伙伴以及媒体有着广泛而深入的合作关系，借助内外部各种资源，目前已建成五大安全网络体系——全球计算机病毒监测网、全球计算机病毒应急处理网、全国计算机病毒预报网、全国反病毒服务网以及全球病毒疫情监测网。

公司总部设立在北京，拥有国内最大的信息安全研发团队、国内最大的客户服务团队，以及销售、市场、网站等部门，并已经建成覆盖全国的庞大的销售和市场体系。

目前瑞星拥有数千万个人用户，数万家企业用户，主要软件产品以中（简、繁体）、英、俄、德、日五种语言版本推向全球市场，销售网络覆盖北美、欧洲、亚太等地区。作为在中关村成长起来的高科技企业，瑞星正逐步走向世界，实现公司的美好愿景——成为全球最具价值的信息安全产品和服务提供商。

附录二 瑞星信息安全资讯网

瑞星信息安全资讯网是全球最大的中文专业信息安全网站，拥有简体中文、繁体中文、日文和英文四个版本，为个人和企业用户提供权威的反病毒和信息安全资讯服务。网站连续两年被评为中国商业网站 100 强，中国最优服务 5 佳网站。

瑞星网站是国内最权威的重大病毒和安全漏洞新闻发布平台，每当出现重大病毒及系统安全漏洞威胁用户安全时，瑞星网站将提供全面的解决方案，包括病毒新闻、最新动态、技术解决方案和免费的专杀工具。同时，网站也提供手机短信息服务，为用户提供更贴身的信息安全保护。

瑞星网站可以为个人和企业用户提供量身订制的信息安全产品和服务，个人用户可以在网站进行免费在线查毒，及时检查自己计算机中是否隐藏着病毒，下载免费杀毒工具和漏洞弥补工具；企业用户可以在网站查找适合自己的信息安全解决方案，在线定购相应产品。

瑞星信息安全资讯网是八千多万瑞星正版用户自己的网站，它是瑞星公司对正版用户的售后服务在网络上的延伸。作为反病毒领域的领先企业，瑞星公司一直致力于不断地自我完善及不断进取之中，为了让您的计算机和存储的宝贵数据高枕无忧，瑞星公司再次提醒您关注瑞星信息安全资讯网站，提醒您不断进行软件的升级更新，避免遭到病毒的侵袭。