瑞星虚拟化系统安全软件
使用手册

北京瑞星信息技术股份有限公司

2017

用户许可协议

重要提示：

在您使用北京瑞星信息技术股份有限公司（以下称“瑞星公司”或“瑞星”）产品（包括但不限于瑞星网络版杀毒软件、瑞星企业终端安全管理系统软件、瑞星虚拟化系统安全软件、瑞星企业移动管理系统软件、其他企业用产品，以下称 “本产品”，具体参见本协议“4 定义 4.1”）之前，请务必仔细阅读本用户许可协议（以下称“本协议”或“EULA”），任何与本协议有关的产品软件、电子文档等都应依照本协议的条款而授权您使用，同时本协议亦适用于任何有关本产品软件的后期发行和升级。您在安装本产品前应仔细阅读本协议的各项条款，尤其需注意免除或者限制瑞星公司责任的免责条款及对用户的权利限制。您保证，在使用本产品之前，已理解并接受本协议。

1. 范围

本协议是您（自然人、法人或其他组织）与本产品的权利人瑞星公司之间就本产品及相关服务事项达成的最终的、完整的且排他的协议。您的雇员或其他代理商，经销商或承建商安装或使用本产品和（或）服务时，亦必须接受本协议后方可使用本产品和（或）服务。试用用户（见本协议“4 定义 4.4”）安装使用本产品，供评估本产品使用，亦须遵守本协议。

2. 协议生效

2.1 您在瑞星官网（www.rising.com.cn）下载安装使用本产品或者注册本产品信息，即表示您同意接受本协议各项条款的约束，本协议生效。

2.2 您通过安装光盘（CD/ DVD）、复制备份软件或者访问等其它方式使用本产品，即表示您同意接受本协议各项条款的约束，本协议生效。

2.3 您在使用试用版或其他版本的产品和（或）服务，即表示您同意接受本协议各项条款的约束，本协议生效。

3. 协议拒绝

如果您不能完全遵守本 EULA 的条件和条款，瑞星公司可以随时终止本 EULA。在此情况下，您必须销毁本产品的所有拷贝及其所有组成部分。

4. 使用的术语和定义

4.1 “本产品”是指：以瑞星公司软件为主要内容的磁盘、光盘、或者是其它介质的所有信息、软件、材料、资料等，包括但不限于瑞星公司或者第三方电脑信息或者软件；

瑞星公司许可您使用的瑞星公司软件的升级程序、修改版本、更新和添加的产品功能以及瑞星公司发布的使用本软件所需相关工具（如果有）；

附带瑞星公司软件的硬件设备，包括但不限于主机、闪存卡、连接器等；

相关的说明性书面材料、产品包装和电子文档；

4.2 “组件服务”：是指购买本产品后会获得相应的产品软件注册服务、软件升级服务、电话支持服务，邮件服务、专家门诊服务、以及硬件上门调试、更换维修等。

4.3 “产品升级”：是指本产品软件开发维护的后续版本，包含 bug 修复或功能上的新增与改进，通常指小数点右侧的版本号的变化。

4.4 “试用用户”：是指没有购买本产品和（或）服务使用许可证的用户，其使用本产品和（或）服务的目的仅作为对产品的试用或评估，一般情况下试用期（评估期）为三十（30）个自然日。

4.5 “付费用户”：是指购买本产品和（或）服务使用许可证的用户。

4.6 “计算机”：是指个人计算机、工作站、手持个人电脑、手机或移动电话或其他数字电子设备。

4.7 “虚拟机”：指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。

4.8 “使用”：指依据文档存取、安装、下载、复制或以其它方式对本产品做功能性使用。

4.9 “用途”指您使用本产品的限制和范围。本产品系瑞星企业级产品，您使用产品的用途限于您及您的员工在企业办公场所内从事日常经营使用，除非经瑞星公司另有书面授权，您不应将该产品授权企业或员工个人在购买企业办公场所以外使用，亦或不得授权非购买企业或其员工使用。

5. 试用用户使用许可

如果您为试用用户，在试用本产品和（或）服务（“一般是评估期起始之日起三十（30）

自然日在非生产环境中使用的软件或服务进行评估或测试的目的”）评估期间，您有权获得电话支持服务、邮件服务、远程专家门诊服务，以及通过访问瑞星官网的形式获得产品更新、内容安全更新和服务更新，当试用期（评估期）结束后，瑞星公司有权终止该产品和（或）服务的使用，同时您必须删除或销毁所有瑞星公司的软件和文档的副本、并归还相关软件载体或硬件设备。

6. 有偿使用许可

作为付费用户，在使用本产品和（或）服务期间，您有如下的权利和义务：

6.1 产品：在您遵守本协议条款和支付相应的许可费的条件下，您可以在授权许可范围。内安装和使用该产品。

6.2 组件服务：在您遵守本协议条款和支付相应的许可费的条件下，可以获得相应的服务支持，如产品软件注册服务、软件升级服务、电话支持服务，邮件服务、专家门诊服务、硬件上门调试、更换维修以及根据与瑞星公司签订的其他协议依法享有的其他服务。

6.3 文档：您可以复制合理数量的副本以供内部培训和使用。但是，所有此类副本必须包含原始文档里瑞星公司的标识信息。

6.4 费用支付：您可以通过现金、支票或者银行转账方式向瑞星公司支付费用。具体的费用支付将由您与瑞星公司另行书面约定。

7. 知识产权

7.1 本产品及瑞星公司授权您制作的任何相关副本均为瑞星公司的产品，其知识产权归瑞星公司所有。本产品的结构、组织和代码均为瑞星公司的有价值的商业秘密和保密信息。本产品受到《中华人民共和国著作权法》、《中华人民共和国著作权法实施条例》及其他相关中国法律法规、规章制度的保护，同时受到国际著作权条约和其他国际知识产权条约的保护。您不得在本协议许可的范围之外复制瑞星公司的软件，否则将构成对瑞星公司知识产权的侵犯。同时，根据本协议您不得对瑞星公司软件进行逆向工程、反编译、反汇编或以其它方式尝试发现瑞星公司软件的源代码，瑞星公司书面授权许可您进行合法反编译的除外。瑞星公司提供的或您获得的有关瑞星公司的任何信息只能由您为本协议许可的目的而使用，不得透露给任何第三方或用于创建任何与瑞星公司软件风格相似的软件，在未经瑞星公司书面授权的情况下不得用作其他商业用途。

7.2 本协议对您使用本产品软件的授权并不意味着瑞星公司对其享有的知识产权做出任何部分或全部的转让。

8. 产品软件使用许可

在遵守本协议的条款的前提下，瑞星公司即授予您非独占性的软件使用许可，允许您依据本协议规定的用途使用本产品软件（包括硬件产品附带的瑞星公司软件）。

8.1 授权使用范围

对单个产品软件，瑞星公司只授权您在一台计算机上使用，但在下列情况下您可以将本产品软件用于多用户环境或网络系统上：

(a) 瑞星公司书面授权许可您用于多用户环境或网络系统上；

(b) 您使用软件的每一节点及终端都已向瑞星公司购买了使用许可。

8.2 复制、分发和传播

您应当按本协议的规定使用或复制瑞星公司产品软件。您必须保证根据本协议授权的每一份复制、分发和传播都必须是完整和真实的，包括所有有关本产品软件的相关软件、电子文档、版权和商标等方面的信息，亦包括本协议。出于备份或档案管理的目的您可以制作一个软件副本，但不可在任何未购买本产品软件使用许可的计算机和/或未经瑞星公司书面授权许可的其他计算机上安装或使用该副本。除经瑞星公司书面授权外，您不得以任何方式将该副本转让或许可给他人使用。

8.3 转让

除非本协议明示许可，您不得以任何方式，包括但不限于租用、出租、再许可或复制等方式，在其它用户的电脑上使用本产品软件的所有或任何部分。但是您可以在同时满足以下全部条件的前提下将本产品软件的使用权转让给其他人：

(a) 您同时将本协议、本产品软件和与本产品软件捆绑或预安装在一起的所有其它软件或硬件（包括所有副本、更新版和先前版本）一并转让给他人；

(b) 您不对任何副本及与本产品软件有关的任何材料、资料、软件等进行留存，包括但不限于您在电脑上存储的备份和副本；

(c) 受让方接受本协议的条款和条件以及您合法购买本产品时接受的任何其他条款和条件。

8.4 本软件引用、利用、使用的相关第三方成果，技术等关联许可，请查看软件许可目录内容并接受。

9. 产品软件注册

为了获得相应服务、产品更新和技术支持，您必须通过网络或者是纸质注册卡的方式向瑞星公司注册并激活软件和服务。注册使我们能够与您联系，以便确保只有有效授权实体接受相应的服务。注册需要一个实体的名称和地址，联系人姓名和联系方式，一个有效的产品序列号，一个有效的电子邮件地址和其他法律通知。注册失败并不会减少您使用本产品的权利，但瑞星公司无法提供接入服务、产品更新或技术支持。

10. 维护/更新的有偿使用许可证

作为有偿使用本产品和（或）服务的用户，您有权要求产品更新和基于网络、电话或者电子邮件技术支持。从瑞星公司或授权经销商购买的软件许可和（或）服务（统称为“维护”）在您购买之日起的一个月内，您必须通过网络（即通过在瑞星官网在线注册）或者纸质注册卡的方式向瑞星公司注册激活软件和（或）服务以便获取您的用户 ID（即使用许可证），从您获取到用户 ID 之日将开始计算首次服务期限（即“定期保养”，具体期限以购买合同为准）。当定期保养维护期限届满后，若要保留该维护权利，您必须从您的供应商（或瑞星公司）购买续保维护服务。否则，您没有维护权利，即不能再享有后续更新软件版本的使用权和相应的服务，瑞星公司有权拒绝提供软件修改后的版本与服务，包括后续版本包含新特性或功能等。若在定期保养维护期限届满后，您中断一段时间之后要求恢复维护的，瑞星公司有权收取除了维修期限届满后逾期维护费外的其它复费；但是若维护中断时间超过一（1）年，您无权要求恢复维护。

11. 同意电子通信

瑞星将通过产品注册中指定联系人的电子邮件地址通知，或将在其网站上张贴通信，包括更新，升级，特殊优惠和定价或其他类似的信息，客户调查反馈（“通讯”）或其他请求。

12. 数据收集

为了给您提供服务和相关的技术支持以及提高软件和（或）服务的功能，除了产品注册信息外，瑞星公司必须处理和存储关于您网络及设备的相关信息（包括但不限于互联网协议

(IP)地址、媒体访问控制(MAC)地址和操作系统版本）。为了改善产品的功能，瑞星公司会定期上传关于产品使用的安装软件，检测到的恶意软件或潜在的不必要的文件的电子信息，您同意瑞星公司进行如下的行为：

（1）为了提高产品的功能和服务的质量，使用已经上传的数据；

（2）与安全合作伙伴共享已经被确认为恶意或者是有害的数据。

13. 备份

在使用任何产品和服务期间，您应当在不同的介质上定期对您的数据和计算机系统进行备份。您理解并知晓在软件、服务或者更新发生错误时，任何一次备份的失败都可能会导致您数据和计算机系统的丢失。由于只有您能执行备份计划以确保在软件、服务或者更新发生错误时，能最大限度的恢复数据和计算机系统，故对您备份的失败，瑞星公司不承担任何责任。

14. 审计

在您正常的工作时间和合理的通知的条件下，瑞星公司有权审核您使用产品和服务的情况。如果审核发现了未经授权的计算机、虚拟机或用户，在接到瑞星公司通知的三十（30）个自然日以内，您应当就未经授权的计算机、虚拟机或用户支付产品许可费。若为未经授权的计算机、虚拟机或用户支付的费用超过审计之前已付费用的 5%，瑞星公司有权要求您赔偿审计所花费的成本和费用。

15. 承诺与责任免除

15.1 瑞星公司向愿遵照本许可协议的条款使用本产品而购买的用户保证，在您购买本产品之日起三十（30）个日历日内，如果本产品自身异常而导致的产品不能正常使用，瑞星公司在经过检测核实后负责更换，但若该异常是因用户错误使用、人为损坏、非法使用、突发事故导致或介质丢失的除外。如依据上述规定要求瑞星公司负责进行更换的，必须在购得本产品后三十（30）个产品日内自费将本产品连同购买凭据退回购买地点，否则视本产品为合格产品。

15.2 瑞星公司保证本产品在正常使用条件下实质上符合其产品说明书中规定的性能要求。

15.3 瑞星公司不对本产品特殊应用目的的商业性和适用性承担保证责任。

15.4 瑞星公司不保证本产品没有错误，或者能够不间断的操作。瑞星公司不保证本产品在任何情况下在任何计算机上均有效。

15.5 您知悉并理解由于防病毒产品软件的特殊性，该软件不可能对于现在或将来的任何病毒均有效。您同意瑞星公司不就因该软件未能防御病毒而发生的损失（包括已通知瑞星公司有可能发生该等损失的情形），包括但不限于营业利润损失、业务中断、业务信息、文档、数据丢失或其他后果性、附带性、间接性经济损失承担赔偿责任，除非该等损失是瑞星公司的故意或欺诈行为造成的。您同意，无论本协议中是否有其他规定，无论在任何情况或根据任何规定，在本协议或与本协议相关的协议履行期间，因瑞星公司造成您或您的相关方发生任何实际损失、或有损失的，瑞星公司对您或您的相关方的最大损失赔偿责任（无论是由于任何违约、侵权或瑞星公司的任何作为或不作为或其他）不应超过 1000 元人民币。

15.6 瑞星公司不对本产品中包含的第三方软件产品的适用性及功能性负责，您在使用本软件产品中遇到的因第三方软件产品引起的故障、损失由该软件产品相关权利人负责，瑞星公司将提供必要的、合理范围内的协助。

16. 用户的声明与保证

16.1 您承诺您具有签署并履行本协议的全部资格、权利、权力、许可及授权；

16.2 您承诺不以任何不合法的方式、为任何不合法的目的、或以任何与本协议不一致的方式使用本产品和相关服务；

16.3 您承诺您通过本软件实施的所有行为均遵守中国（为本协议之目的，不包含香港特别行政区、澳门特别行政区和台湾地区）法律、法规和相关规定以及各种社会公共利益或公共道德。如有违反导致任何争议、纠纷等不利后果的发生，您将以自己的名义独立承担所有相应的法律责任。

16.4 您同意，因您违反本协议或经在此提及而纳入本协议的其他文件，或因您违反了相关法律法规、国家政策等或侵害了第三方的合法权利，而使第三方对瑞星公司或瑞星公司的职员、代理人提出索赔要求（包括但不限于司法费用和其他专业人士的费用），您必须对瑞星公司及瑞星公司的职员、代理人由此遭受的全部损失承担赔偿责任。

16.5 您承诺，未经瑞星公司书面许可，因签署、履行本协议而获知的有关瑞星公司任何形式的非公开信息（包括但不限于技术秘密、商业计划、商业秘密等）均不得向任何第三方

（但为履行本协议而必须知晓的员工除外）公开，否则瑞星公司有权选择以下任意一种方式要求您承担责任；本协议终止的，不影响本款的效力。

（1）要求您支付许可费的 30%作为违约金；

（2）要求您赔偿瑞星公司全部的损失。

17. 协议终止

如果您未能遵守本协议的任何规定，瑞星公司有权随时终止授予您的对本产品的使用许可。终止许可后，您应在瑞星公司通知后，按照瑞星公司的要求处理本产品。

18. 其他

18.1 本协议所定的任何的部分或全部无效者，不影响其他条款的效力。

18.2 本协议的解释、效力及纠纷的解决均适用于中国（为本协议之目的，不包含香港特别行政区、澳门特别行政区和台湾地区），并不考虑法律冲突。

18.3 有关本协议的任何争议应由您与瑞星公司秉承善意友好协商解决。若协商不成，您与瑞星公司均同意将纠纷或争议提交北京仲裁委员会依据当时有效的仲裁规则在北京仲裁解决。仲裁裁决是终局的，对双方均有法律约束力。除非仲裁裁决另有规定，仲裁费用应由仲裁败诉方承担。

18.4 如果您对本协议有任何疑问或者希望从瑞星公司获得任何信息，请按下列地址和方式与瑞星公司联系。

地址：北京市海淀区中关村大街 22 号中科大厦 1403 室

邮编： 100190

网站： http://www.rising.com.cn

电话： 400-660-8866(免长途话费)或(8610)82616666

目 录

1 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. 《快速使用指南》：指导用户快速掌握软件安装、设置及使用的方法。
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. 《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 Server 2003 SP2以上（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及以上、Firefox、Google Chrome、Safari

b. 硬件和网络要求

CPU：1GHz以上

内存：4GB以上

硬盘空间：10GB以上

网络环境：100M以上网络，需一个固定IP地址

1.2.2 日志中心

a. 软件环境

1）操作系统

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

Windows Vista（32-bit、64-bit）

Windows Server 2008（32-bit、64-bit）

Windows Server 2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：1GHz以上

内存：2GB以上

硬盘空间：10GB以上

1.2.3 升级中心

a. 软件环境

1）操作系统

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

Windows Vista（32-bit、64-bit）

Windows Server 2008（32-bit、64-bit）

Windows Server 2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：1GHz以上

内存：2GB以上

硬盘空间：10GB以上

1.2.4 VMware 无代理杀毒（vShield）

1.2.4.1 安全虚拟设备

a. 软件环境

1）操作系统

VMware vCenter 5.1.0以上

ESXi 5.1.0

2）其它

额外的VMware工具：VMware Tools、VMware vShield Manager、VMware vShield Endpoint Security 5.1（ESXi5 patch ESXi500-201109001 for vShield Endpoint Driver）

VMware Endpoint Protection支持的操作系统：Windows XP SP2 以上（32-bit）、Windows 2003 SP2 以上（32-bit、64-bit）、Windows Vista（32-bit、64-bit）、Windows 7（32-bit、64-bit）、Windows 2008（32-bit、64-bit）。（对于最新支持的客户机平台请参考VMware官网http://www.vmware.com/cn相关介绍）

b. 硬件和网络要求

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

内存：2GB以上，内存容量需求取决于安全虚拟设备保护的虚拟机数量，详情请参考本文档章节3.2.4.3 安全虚拟设备推荐配置

硬盘空间：20GB以上

1.2.4.2 RSTools

a. 软件环境

1）操作系统

Windows XP SP2以上（32-bit、64-bit）

Windows Server 2003以上（32-bit、64-bit）

Windows Vista（32-bit、64-bit）

Windows Server 2008（32-bit、64-bit）

Windows Server 2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：1GHz以上

内存：2GB以上

硬盘空间：10GB以上

1.2.5 VMware 无代理杀毒（NSX）

1.2.5.1 安全服务虚拟机

a. 软件环境

1）操作系统

VMware vCenter 6.5

VMware ESXi 5.5 / 6.0 / 6.5

VMware NSX 6.2.4 / 6.3.0

2）其它

额外的VMware工具：VMware Tools

b. 硬件和网络要求

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

内存：2GB以上，内存容量需求取决于安全服务虚拟机保护的虚拟机数量，详情请参考本文档章节3.2.4.3 安全虚拟设备推荐配置

硬盘空间：20GB以上

1.2.5.2 RSTools

a. 软件环境

1）操作系统

Windows XP (SP2 or later) with Tools version 10.1

Windows Vista (32bit)

Windows 7 (32/64bit)

Windows 2003 SP2 以上 (32/64bit)

Windows 2003 R2 (32/64bit)

Windows 2008 (32/64bit)

Windows 2008 R2 (64bit)

Windows 2012 (64bit)

Windows 2012 R2

Windows 8 / 8.1

Windows 10

RHEL 7 GA (64 bit)

SLES 12 GA (64 bit)

Ubuntu 14.04 LTS (64 bit)

b. 硬件和网络要求

CPU：1GHz以上

内存：2GB以上

硬盘空间：10GB以上

1.2.6 HUAWEI 无代理杀毒

1.2.6.1 安全虚拟设备

a. 软件环境

1）操作系统

华为 VRM 4.0.0以上

CNA-R5

2）其它

额外的华为工具：华为 Tools。

华为Tools支持的操作系统：Windows XP SP2以上（32-bit）、Windows Server 2003（32-bit、64-bit）、Windows Vista（32-bit）、Windows 7（32-bit）、wWindows Server 2008（64-bit）。（对于最新支持的客户机平台请参考华为官网http://www.huawei.com/cn相关介绍）

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

内存：2GB以上，内存容量需求取决于安全虚拟设备保护的虚拟机数量，详情请参考本文档章节3.2.5.2 安全虚拟设备推荐配置

硬盘空间：20GB以上

1.2.6.2 RSTools

a. 软件环境

1）操作系统

Windows XP SP2以上（32-bit、64-bit）

Windows Server 2003（32-bit、64-bit）

Windows Vista（32-bit、64-bit）

Windows Server 2008（32-bit、64-bit）

Windows Server 2008 R2（64-bit）

Windows 7（32-bit、64-bit）

b. 硬件和网络要求

CPU：1GHz以上

内存：2GB以上

硬盘空间：10GB以上

1.2.7 安全防护终端

1.2.7.1 软件环境

1）Microsoft Windows家族。包括：

Windows 2000 Professional

Windows XP Professional/Home Edition

Windows Vista

Windows 7

Windows 8

Windows 8.1

Windows 10

1.2.7.2 硬件环境

剩余磁盘空间：4GB以上

CPU：1GHz以上

内存：2GB以上，最大支持4GB

1.2.8 全功能安全防护客户端

1.2.8.1 软件环境

1）Microsoft Windows家族。包括：

Windows 2000 Professional

Windows XP Professional/Home Edition

Windows Vista

Windows 7

Windows 8

Windows 8.1

Windows 10

1.2.8.2 硬件环境

剩余磁盘空间：4GB以上

CPU：1GHz以上

内存：2GB以上，最大支持4GB

1.2.9 安全终端 Linux 杀毒

1.2.9.1 软件环境

安全终端Linux杀毒支持目前主流的UNIX/Linux操作系统，支持如下UNIX/Linux版本：

SUN Solaris系列

IBM AIX系列

Linux系列：基于Intel x86芯片（例如Redhat Linux、红旗Linux、Ubuntu Linux等）

HP-UX系列：PA-RISC系列

FreeBSD系列

1.2.9.2 硬件环境

支持的硬件环境：

CPU	操作系统
POWER-PC	AIX（5.1、5.2、5.3）
SPARC	SOLARIS（6.0、7.0、8.0、9.0）
PARISC	HPUX（11 系列）
INTEL	Linux（2.4 和 2.6 内核）

图表 1-1 硬件环境

剩余磁盘空间：空闲空间应不小于10GB

CPU：1GHz以上

网络环境：100Mbps及以上网络，需一个固定IP地址

1.2.10 Linux 全功能防护客户端

1.2.10.1 软件环境

Linux/UNIX 操作系统，如中标麒麟、RedHat、SUSE Linux、CentOS 等。

1.2.10.2 硬件环境

CPU：酷睿 2 代 2.5GHz 及以上

内存：2GB 及以上

剩余硬盘空间：4GB 及以上

网络环境：100Mbps 及以上网络，需一个固定 IP 地址

2 软件概述

瑞星虚拟化系统安全软件采用流行的 B/S、C/S 混合架构进行设计，为用户物理网络环境和虚拟网络环境提供完整的安全防护体系。本产品由管理中心、日志中心、升级中心、VMware 无代理杀毒、HUAWEI 无代理杀毒、安全防护终端、全功能安全防护终端、安全终

端 Linux 杀毒和 Linux 全功能防护客户端等子系统组成，各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，共同完成企业内部的安全防护。

管理中心：（PMC）是瑞星新一代的管理控制中心，其既可管理传统的物理客户端，也可管理虚拟机客户端，客户端既包括 Windows，又包括 Linux。它作为管控服务器，一方面为管理员提供统一的管理界面交互，另一方面负责为客户端提供策略、任务、授权等业务数据；是管理员集中设置安全策略，控制客户端授权，定制客户端扫描查杀任务，查看客户端扫描结果，病毒日志，感染趋势报表等功能的管理控制平台。

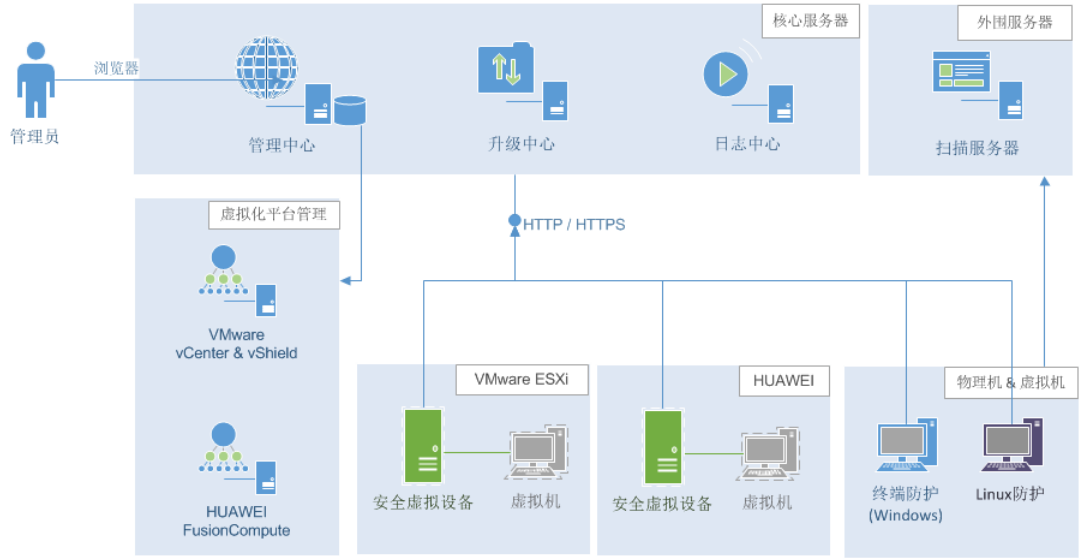
日志中心：接收各客户端产生的日志数据，统一进行入库操作，并负责之间的数据同步；

升级中心：在企业内部为所有客户端提供 http 方式的升级服务，以减轻客户端对互联网的依赖；自身同时支持手动与自动方式升级；

安全虚拟设备：存在于每一台虚拟主机上（如 ESXi），为其上的每一台无代理虚拟机提供安全防护服务，不需要被保护的虚拟机再安装安全产品；

安全终端防护与安全终端 Linux 杀毒：终端安全类子产品，支持 Windows 与 Linux 系统，主要安装在物理机上，也支持安装在虚拟机上，此时将接管无代理安全防护；

瑞星虚拟化系统安全软件支持对虚拟化环境与非虚拟化环境的统一管控，管理员可以对 VMware vSphere / HUAWEI Fusion Sphere 环境内的虚拟机和物理设备进行一致化管理。系统工作时，管理员按需为终端设定策略与任务，各终端连接管理中心后得到相关信息，按管理员的设置参数工作，并将产生的安全业务日志上报到日志中心。



图表 2-1 产品架构图

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，跟踪终端和物理机内的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、华为 VRM 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终端系统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，安全管理员可轻松的、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；

终端和物理机的安全配置与管理；

自定义个性化版面配置；

与 VMware vCenter、华为 VRM 和 Microsoft Active Directory 等管理系统的联动与集成。AD 域终端跟物理机一样，连接到管理控制台之后，直接显示在剩余分组里面。

内建安全

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，避免非授权人员使用而引发的安全风险；

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 日志中心

瑞星虚拟化系统安全软件日志中心可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。

2.3 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、RSTools、安全终端 Linux 杀毒、安全防护终端等子系统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。

2.4 VMware 无代理杀毒（vShield）

2.4.1 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，并保护同一个 ESXi Server 上的其他虚拟机，且每个安全虚拟设备均可拥有各自的安全策略。

病毒防护

瑞星虚拟化系统安全软件需配合 VMware vShield Manager Endpoint Security 使用，才可实现病毒安全防护功能。

当安全虚拟设备检测到病毒时，可以生成警报，当被保护终端安装有 RSTools 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。

2.4.2 RSTools

瑞星虚拟化系统安全软件 RSTools 是轻量化高性能组件，可选安装在被保护的终端上，配合安全虚拟设备实现杀毒提示信息及自动恢复隔离文件的操作。

2.5 VMware 无代理杀毒（NSX）

2.5.1 安全服务虚拟机

瑞星虚拟化系统安全软件安全服务虚拟机（SVM）作为 VMware 虚拟机运行，并保护同一个 ESXi Server 上的其他虚拟机，且每个 SVM 均可拥有各自的安全策略。

病毒防护

瑞星虚拟化系统安全软件需配合 VMware NSX Guest Introspection 使用，才可实现病毒安全防护功能。

当安全服务虚拟机检测到病毒时，可以生成警报，当被保护终端安装有 RSTools 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。

2.5.2 RSTools

瑞星虚拟化系统安全软件 RSTools 是轻量化高性能组件，可选安装在被保护的终端上，配合安全虚拟设备实现杀毒提示信息及自动恢复隔离文件的操作。

2.6 HUAWEI 无代理杀毒

2.6.1 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华为虚拟机运行，并保护同一 CNA 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，当被保护终端安装有 RSTools 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。

2.6.2 RSTools

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终端上，配合安全虚拟设备实现杀毒提示信息及自动恢复隔离文件的操作。

2.7 安全防护终端

安全防护终端是专门为安全解决方案 Windows 系统设计的防病毒子系统。它利用其有效的病毒查杀对 Windows 病毒进行防范和查杀。它既可以按照本机管理员的操作和设置进行病毒扫描和查杀，又可以响应瑞星虚拟化系统安全软件管理中心发出的远程控制指令，作为瑞星虚拟化系统的 Windows 客户端运行，将查杀结果和查杀日志上报虚拟化系统管理中心，方便管理员分析虚拟化安全系统内所有计算机的病毒情况。

2.8全功能安全防护客户端

全功能安全防护客户端是专门为安全解决方案 Windows 系统设计的防病毒子系统。借助先进的多引擎技术以及亿级病毒库的支持，它可有效防范、查杀各类 Windows 木马、病毒及风险程序；同时具备高效、全方位的网络安全防范技术，可提供防火墙、入侵防御（IDS/IPS）、虚拟补丁(Vpatch)、防 Sql 注入等安全功能。

2.9 安全终端 Linux 杀毒

安全终端 Linux 杀毒是为安全解决方案 Linux 系统设计的防毒子系统，可对 Linux 病毒进行防范和查杀。它既可以按照本机管理员的操作和设置进行病毒扫描和查杀，又可以响应瑞星虚拟化系统安全软件管理中心发出的远程控制指令，作为瑞星虚拟化系统的 Linux 客户端运行，将查杀的结果和查杀日志传送到虚拟化系统管理中心，便于网络管理员了解瑞星虚拟化系统网络内的所有计算机的病毒感染情况。

2.10 Linux 全功能防护客户端

瑞星杀毒软件 for Linux 为中标麒麟、RedHat、SUSE Linux、CentOS 等多种主流企业级 Linux 系统提供安全防护，主要包括四大功能，分别为：病毒查杀、文件监控、网络监控和安全工具。

2.10.1 病毒查杀

病毒查杀是瑞星杀毒软件 for Linux 的基础功能，主要实现系统文件病毒查杀、病毒防护，可以实现快速查杀、自定义查杀以及全盘查杀，同时，可以进行查杀设置，隔离病毒文件，添加可信文件。整个操作界面基本保持了 Windows 版本杀毒软件的样式，用户使用习惯上也基本一致。

2.10.2 文件监控

瑞星杀毒软件 for Linux 文件监控是功能强大的文件监控系统，开启监控后，可以时刻保护文件的安全。通过对进程读取文件行为的监控，及时发现敏感文件的修改，当检测到病毒后，自动为用户激活查杀功能并处理病毒文件，阻止病毒感染更多文件。

2.10.3 网络监控

瑞星杀毒软件 for Linux 网络监控开启后，可以及时发现网络异常和风险，对非常依赖网络的 Linux 系统尤为重要。用户设置需要监控的应用或者进程后，网络监控即可开始实时监控相应的网络事件。

2.10.4 安全工具

瑞星杀毒软件 for Linux 安全工具提供了一些方便的附加工具，如网址导航、安全团购、

网站安全监测和瑞星智能服务。

3 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RSTools、安全虚拟设备、安全防护终端、全功能安全防护客户端、安全终端 Linux 杀毒和 Linux 全功能防护客户端。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它对象。

注意：各个终端部署存在互斥关系，安全防护终端与全功能安全防护客户端互斥，安全终端Linux杀毒与 Linux全功能防护客户端互斥。

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

安全防护终端

- 通信：29037

安全虚拟设备

- 通信：5557

安全终端 Linux 杀毒

- 通信：5557

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虚拟化产品官方网站（rvs.rising.com.cn）注册生成服务号，再使用服务号登录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。

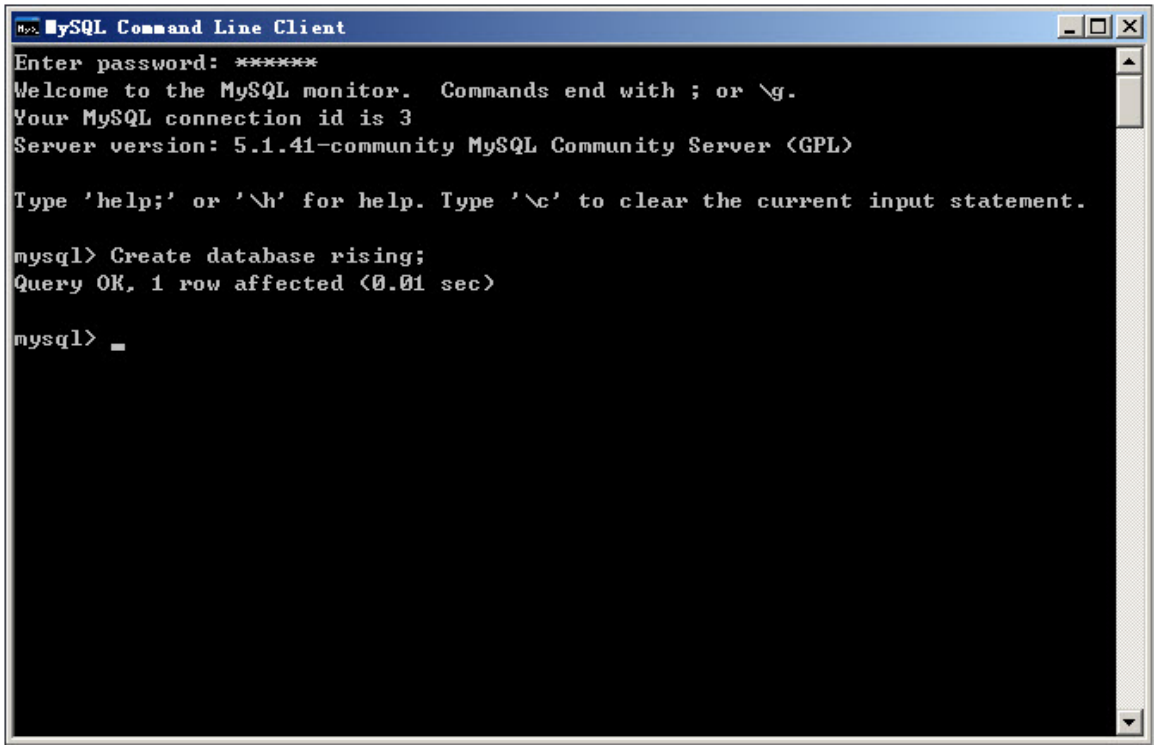
提示：您还需要获取VMware相关组件的激活码，如使用瑞星虚拟化系统安全软件杀毒功能必须获得VMware vShield Endpoint Security 5.1激活号。

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，所以要保证各子系统的主机名或 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

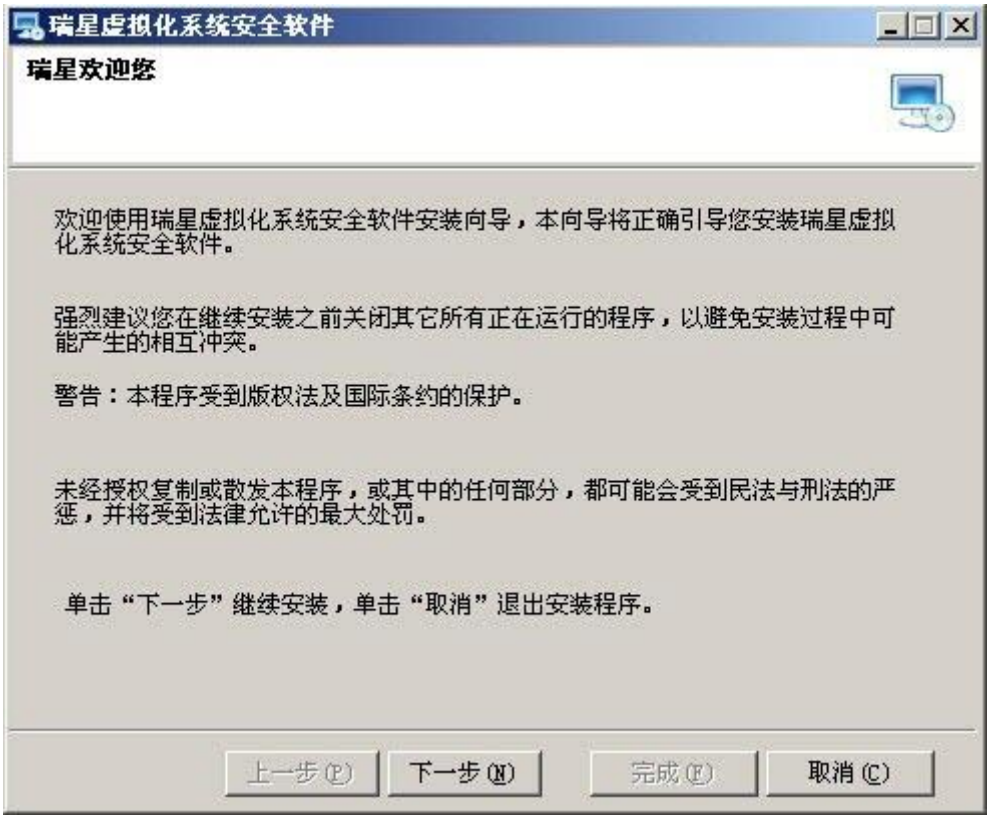
3.2 组件安装

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，点击 PMC_unified.exe 启动产品安装主界面后，开始安装。

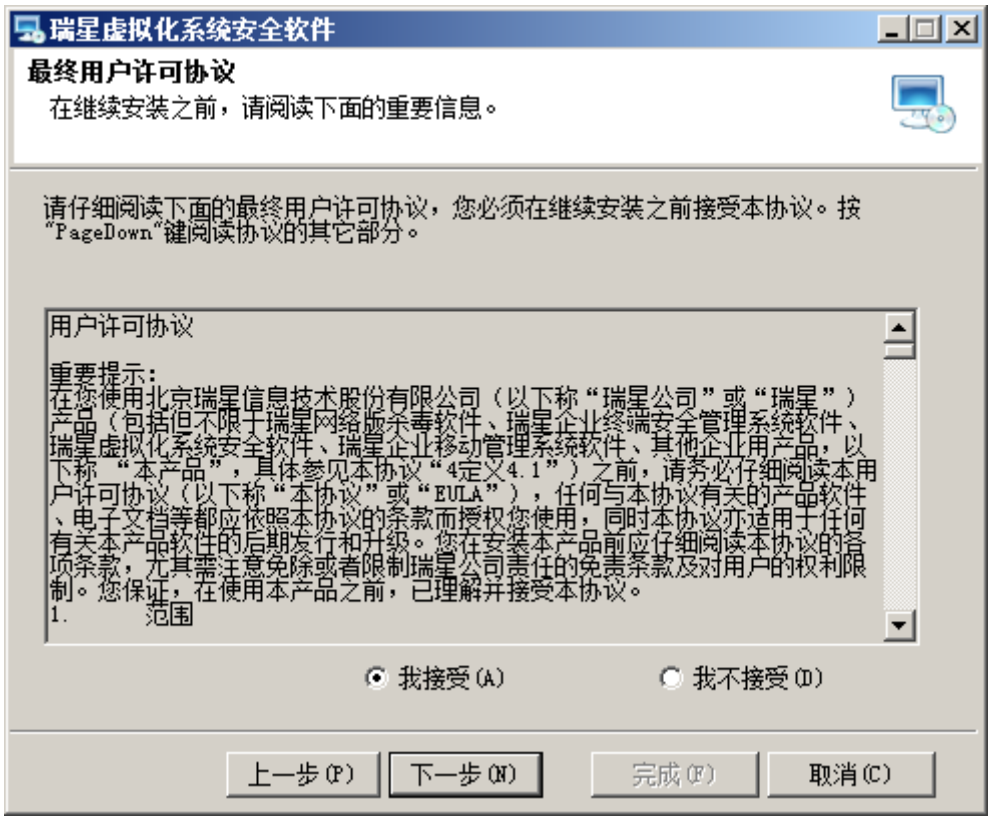
图表 3-2

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。



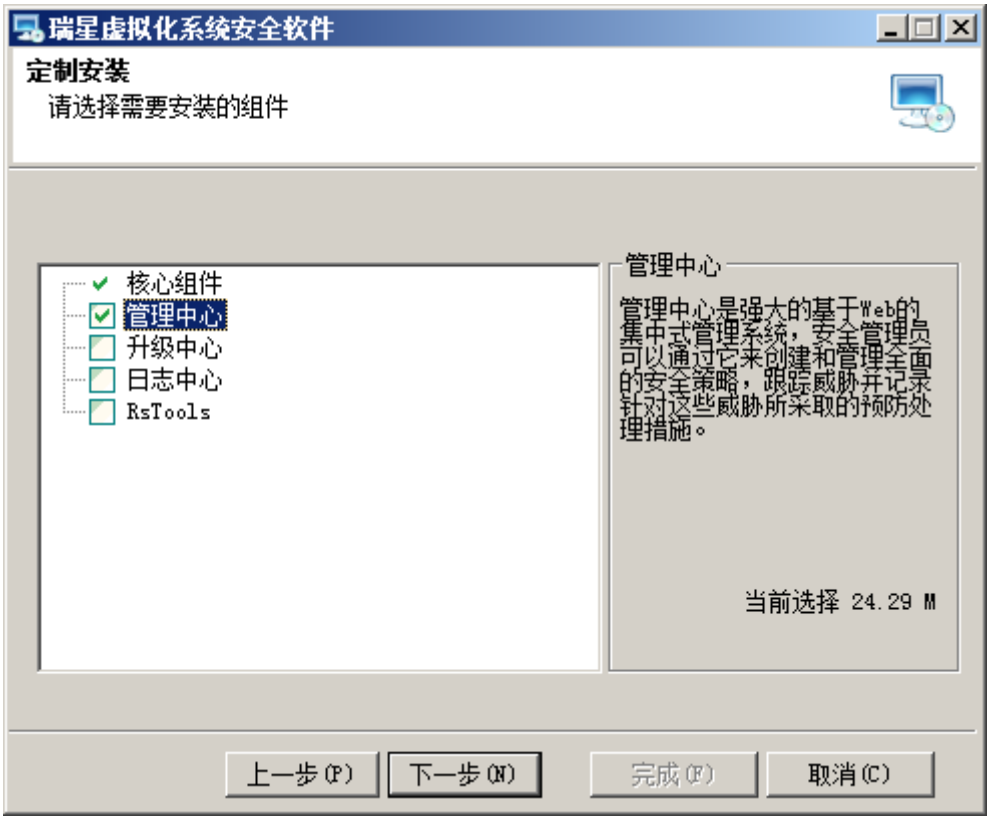
图表 3-3

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】界面显示设定管理中心参数，点击【下一步】继续安装。

图表 3-8

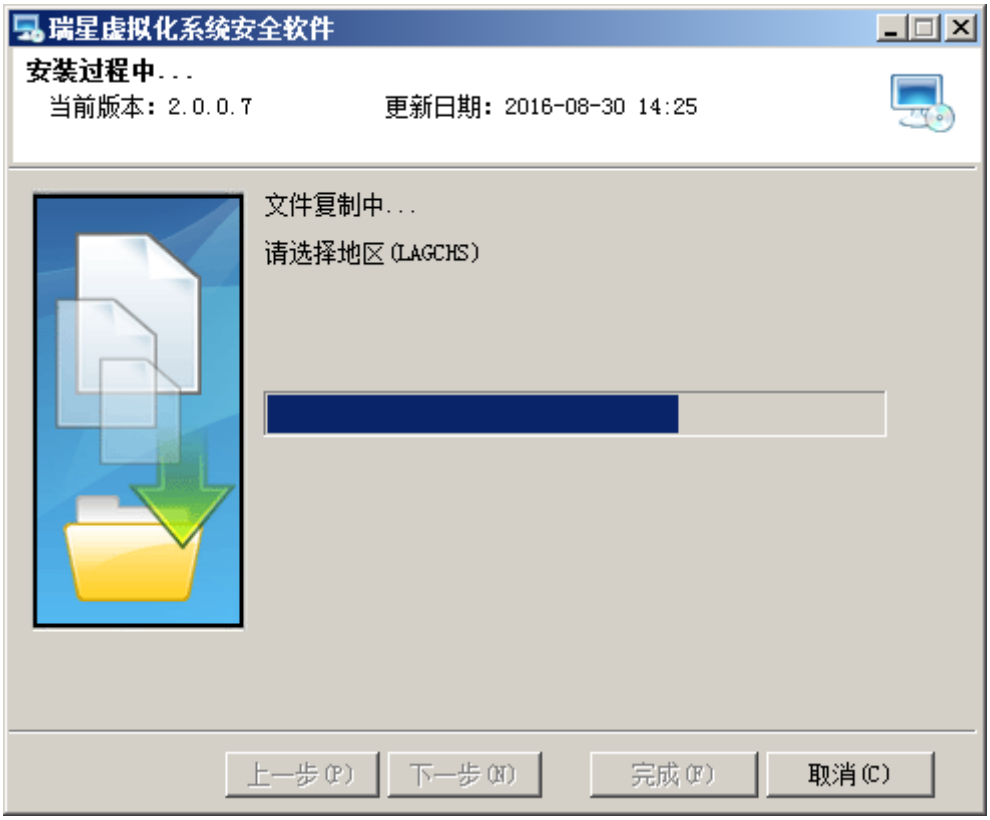
第八步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。

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。

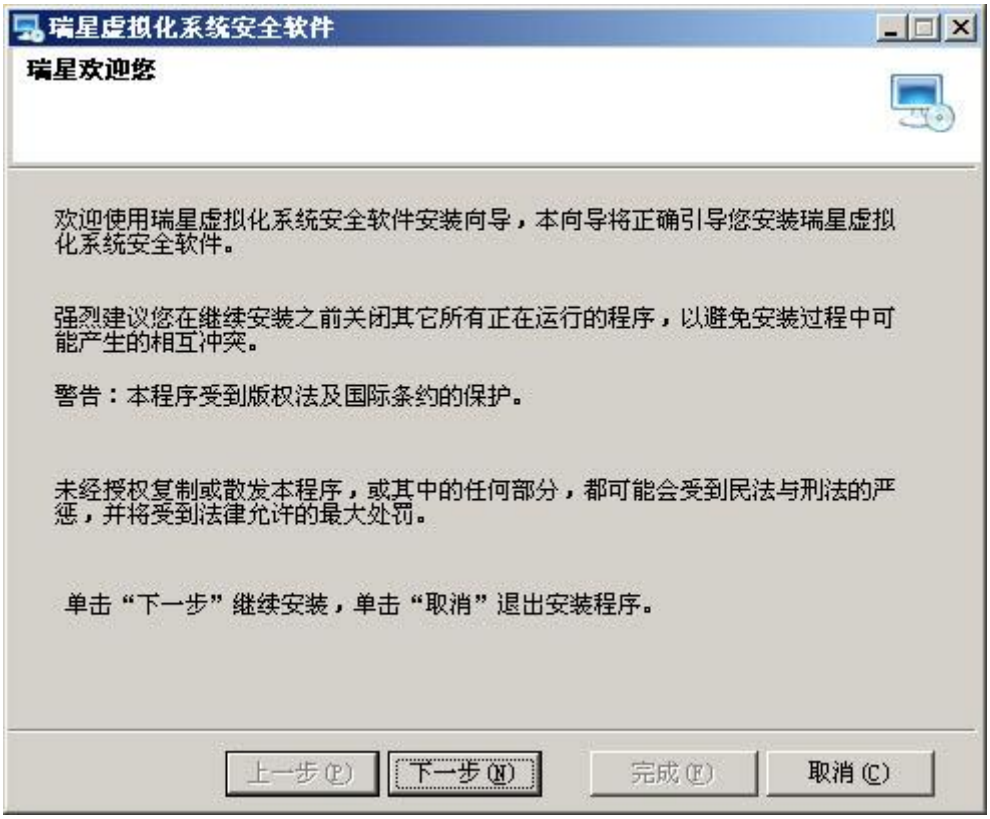
图表 3-12

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，点击 PMC_unified.exe 启动产品安装主界面后，开始安装。

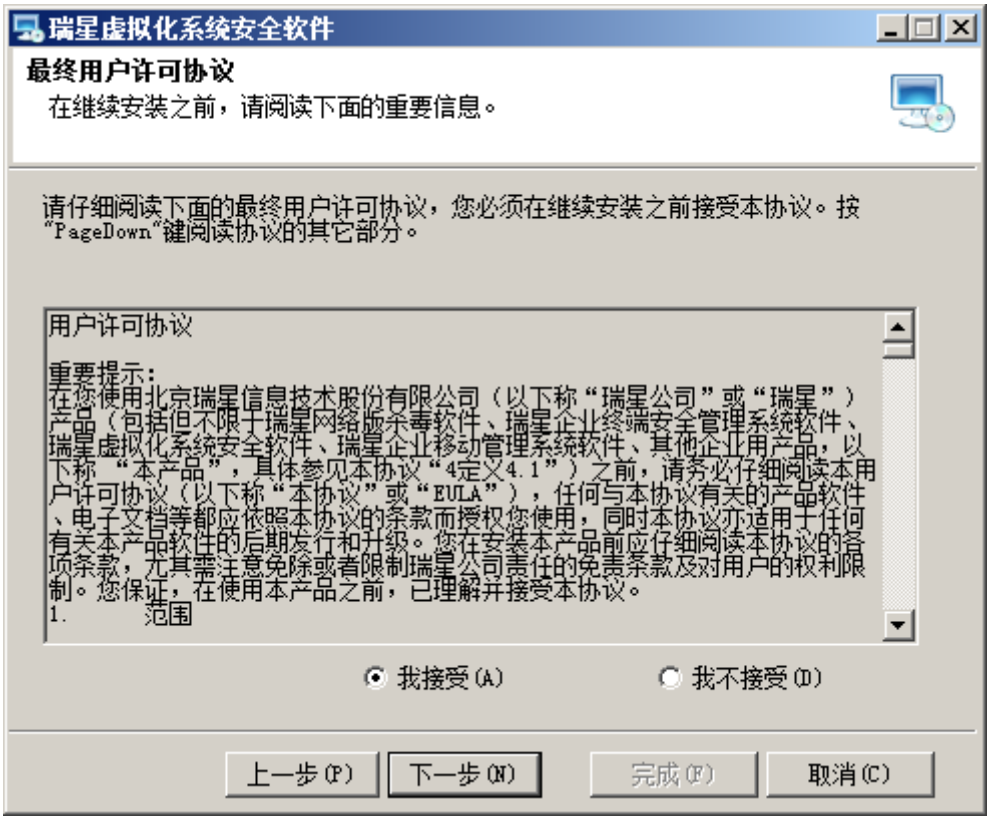
图表 3-13

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。



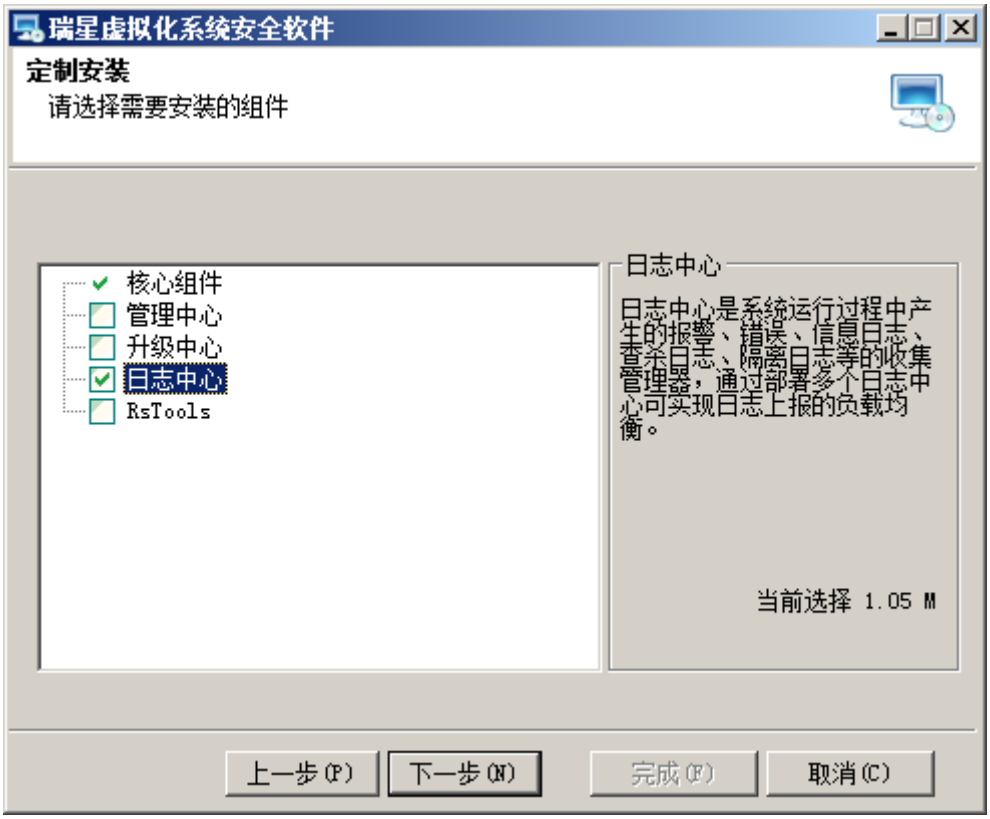
图表 3-14

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】界面显示设定客户端参数，点击【下一步】继续安装。

图表 3-17

第六步：在【日志中心选项】界面显示设定日志中心参数，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

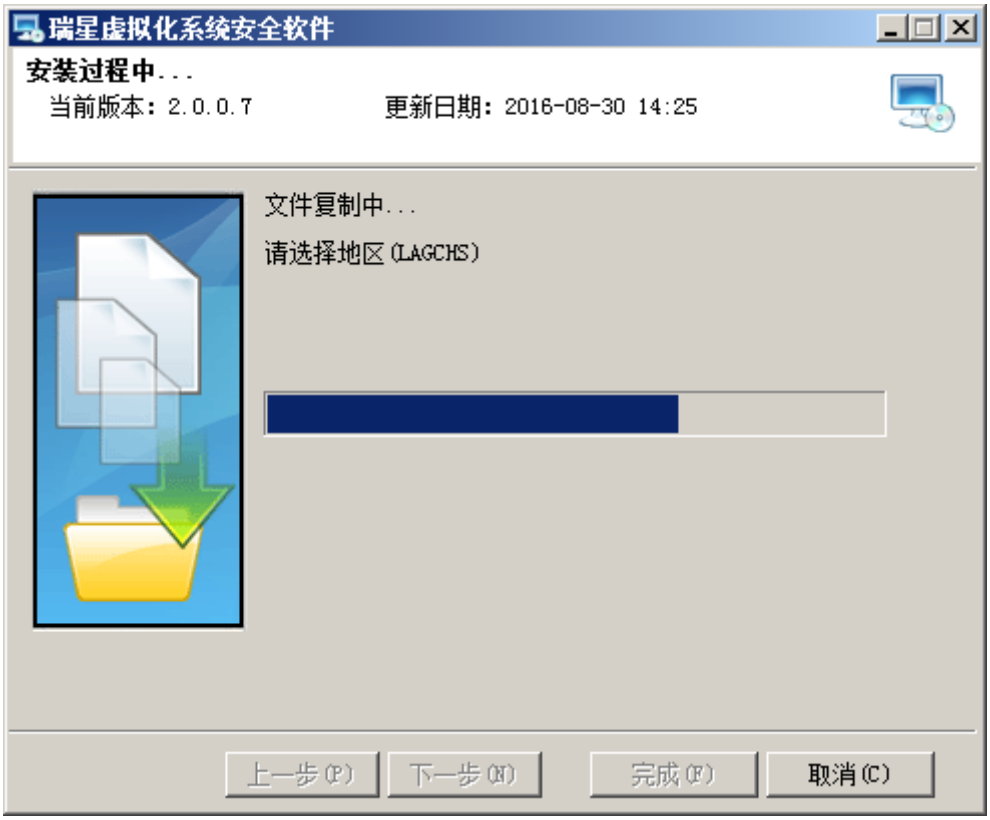
第八步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。

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。

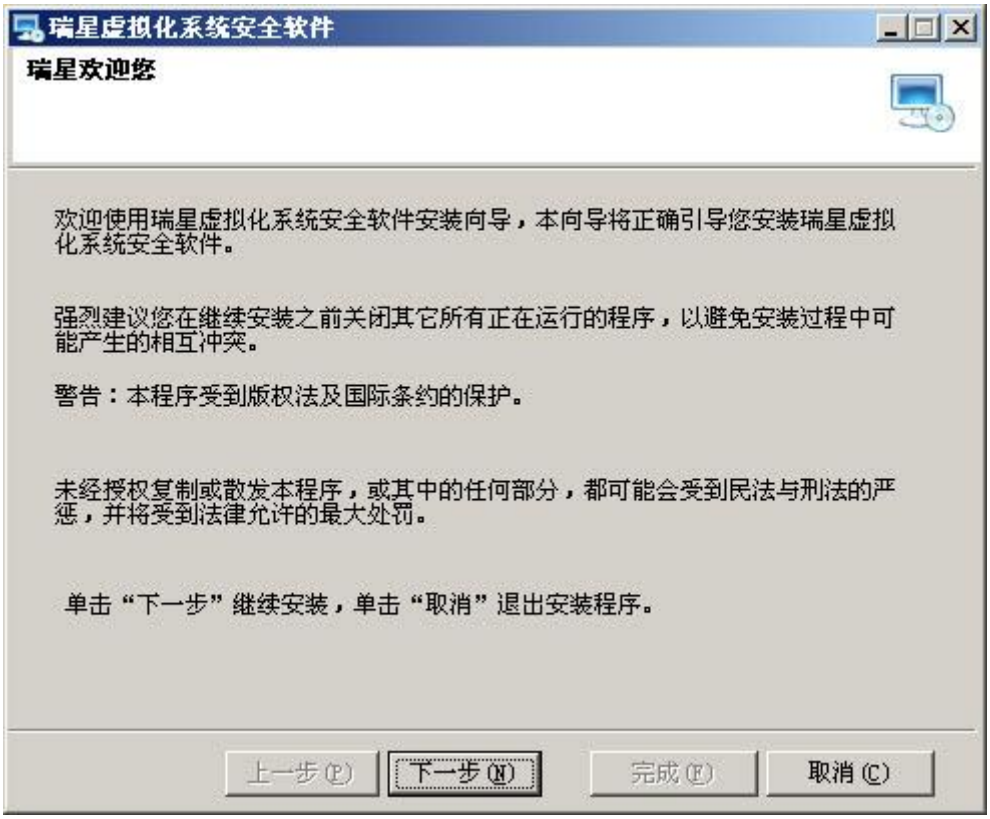
图表 3-23

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，点击 PMC_unified.exe 启动产品安装主界面后，开始安装。

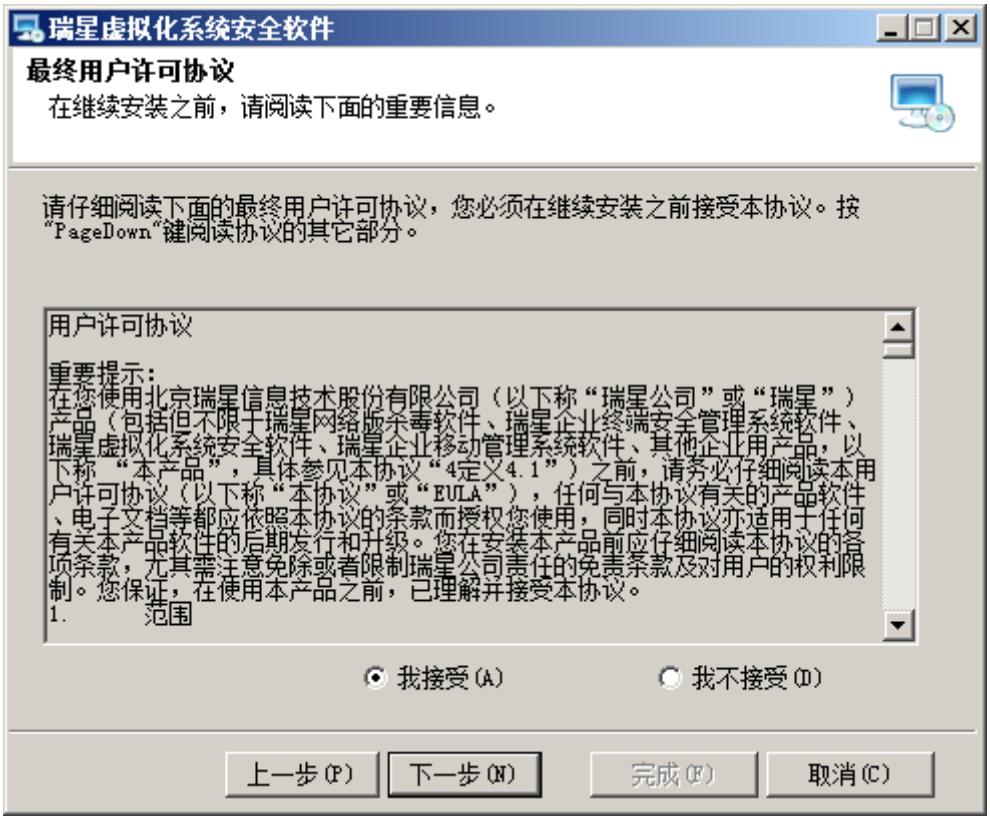
图表 3-24

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。



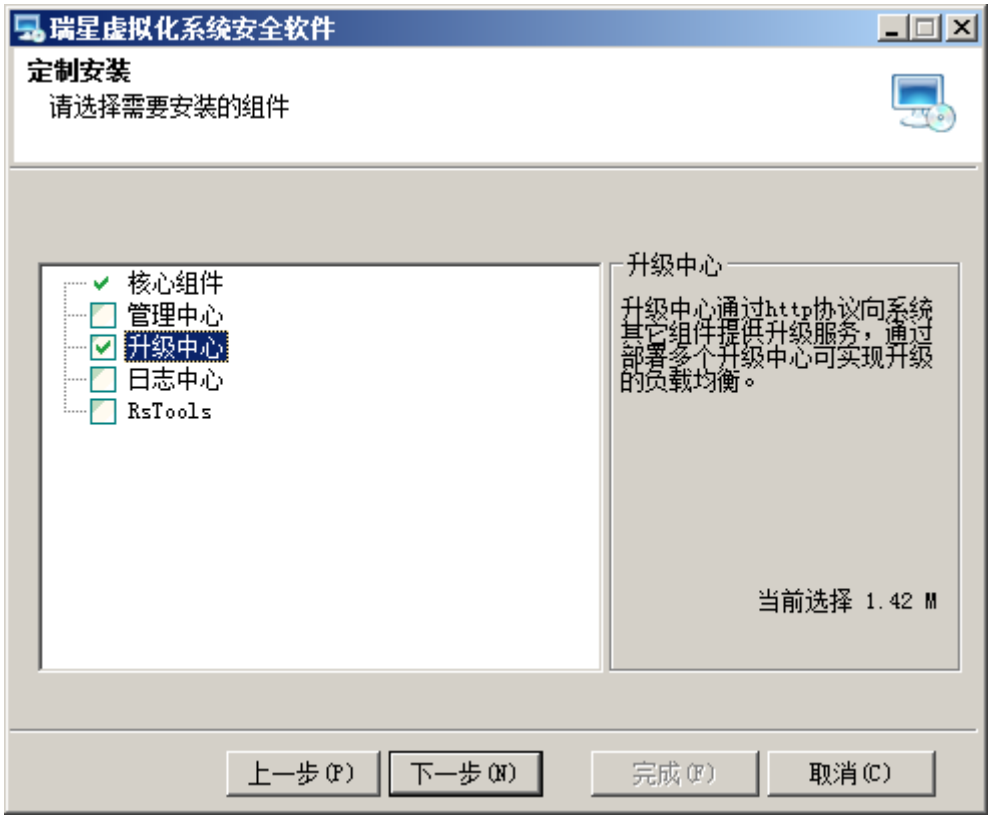
图表 3-25

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】界面显示设定客户端参数，点击【下一步】继续安装。

图表 3-28

第六步：在【升级中心选项】界面显示设定升级中心参数，点击【下一步】继续安装。

图表 3-29

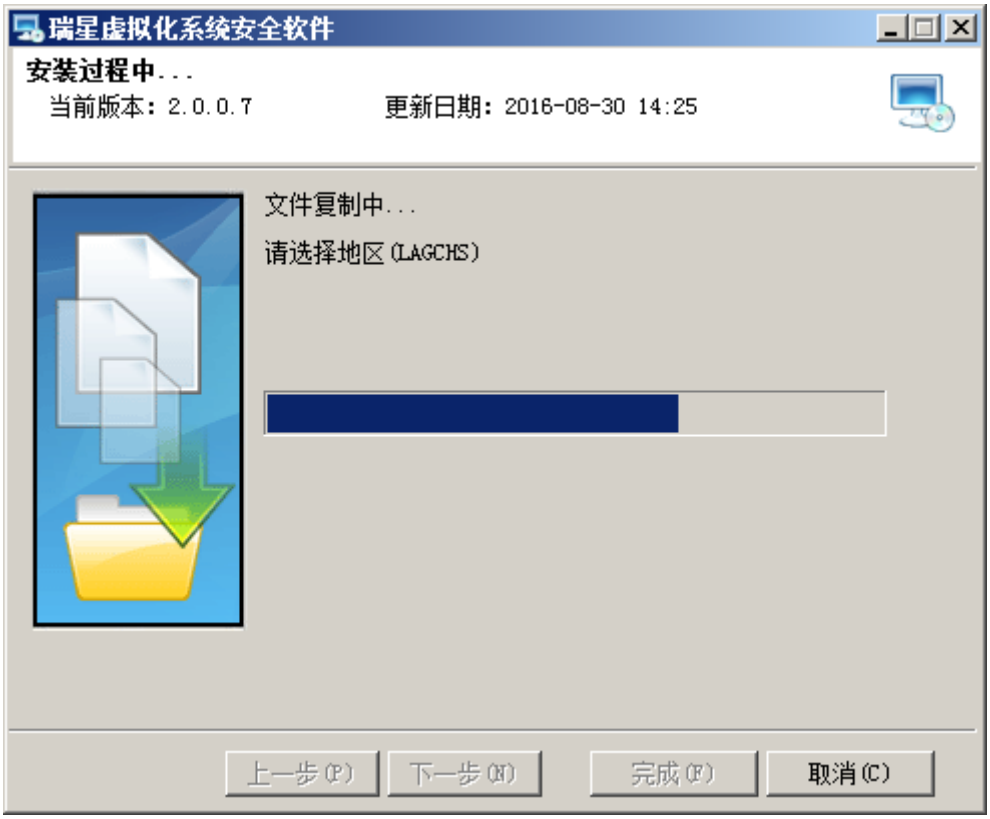
第七步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。

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

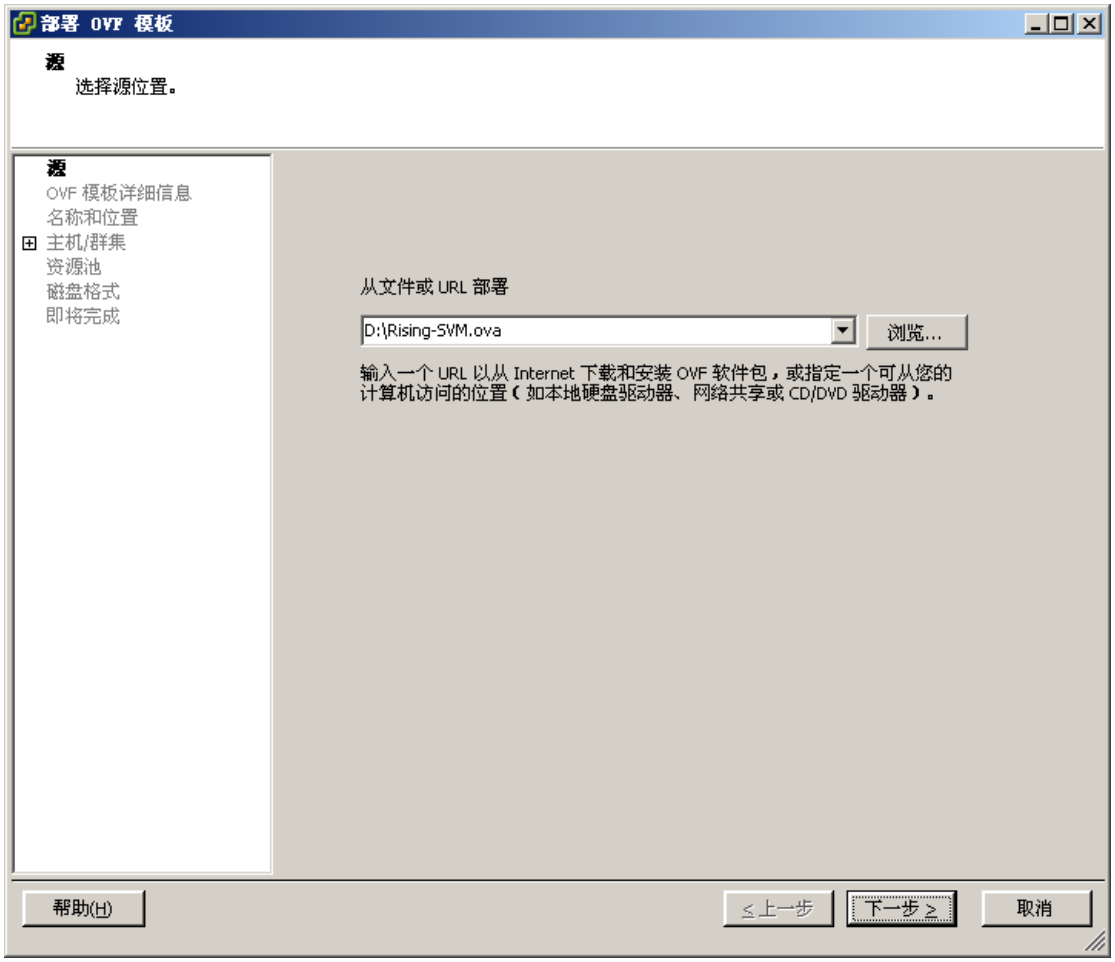
3.2.4 VMware 无代理杀毒（vShield）

3.2.4.1 安全虚拟设备

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

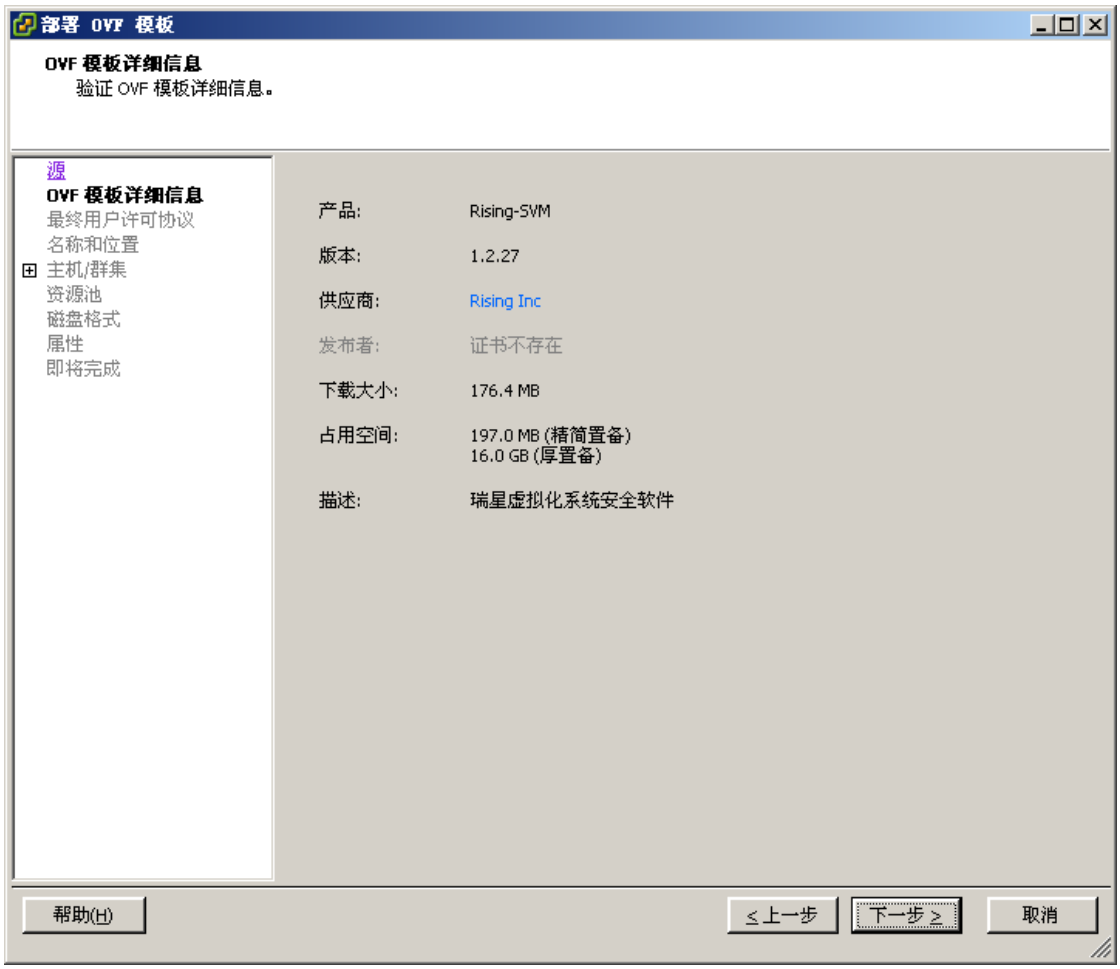
图表 3-34

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。



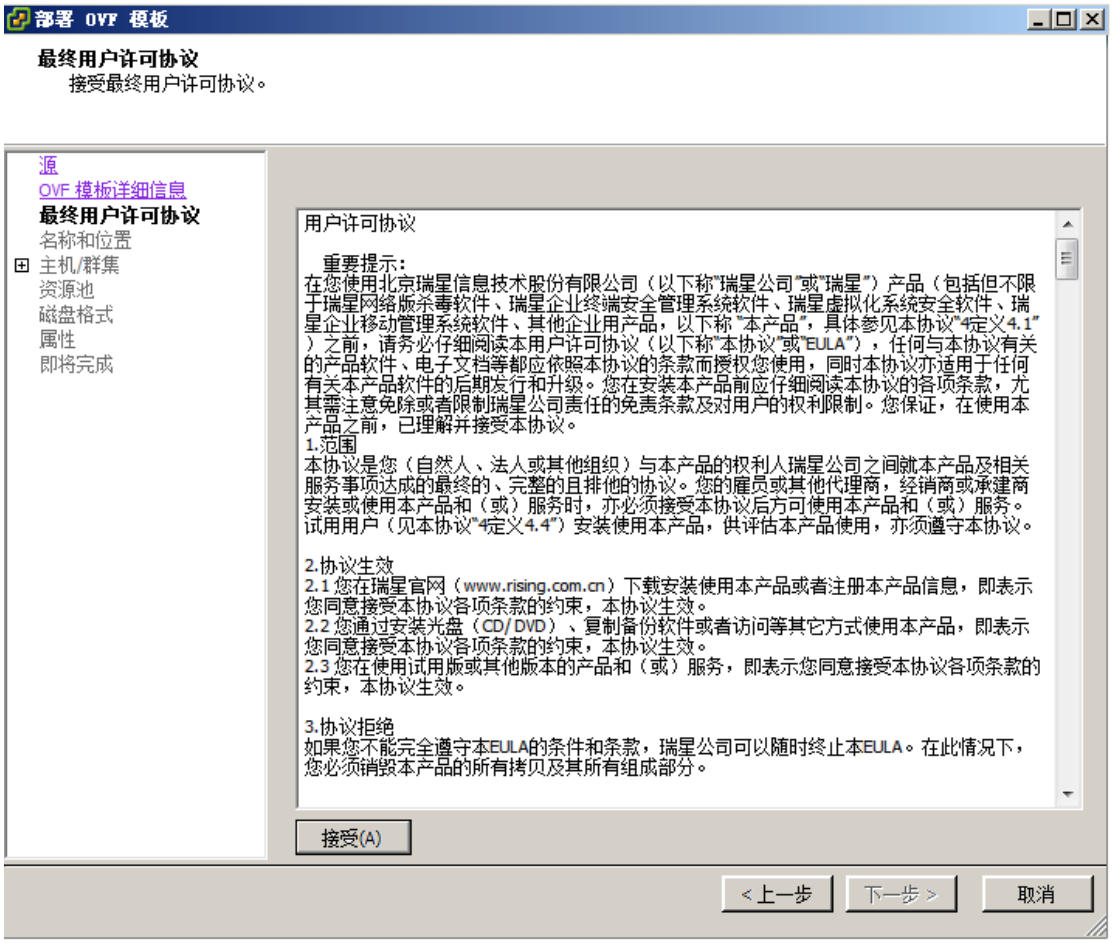
图表 3-35

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。



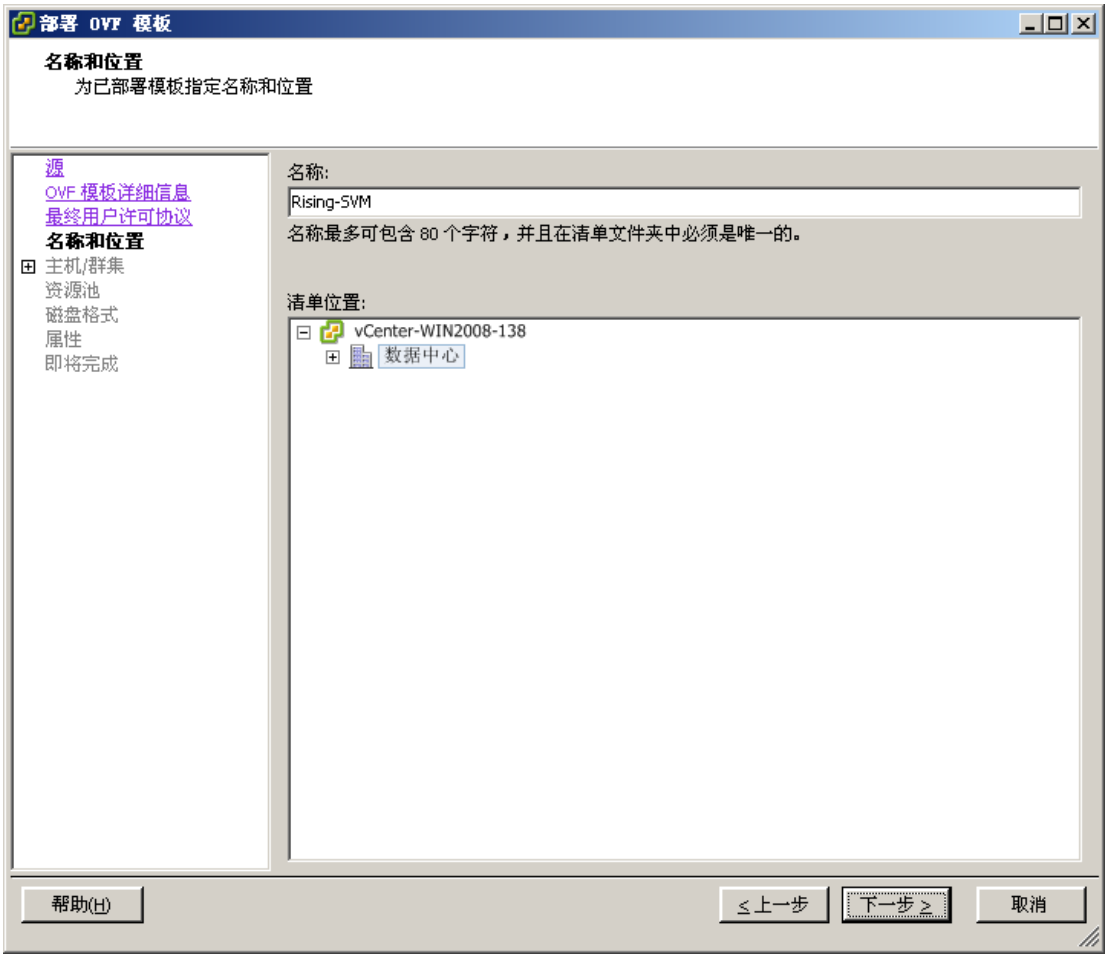
图表 3-36

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。



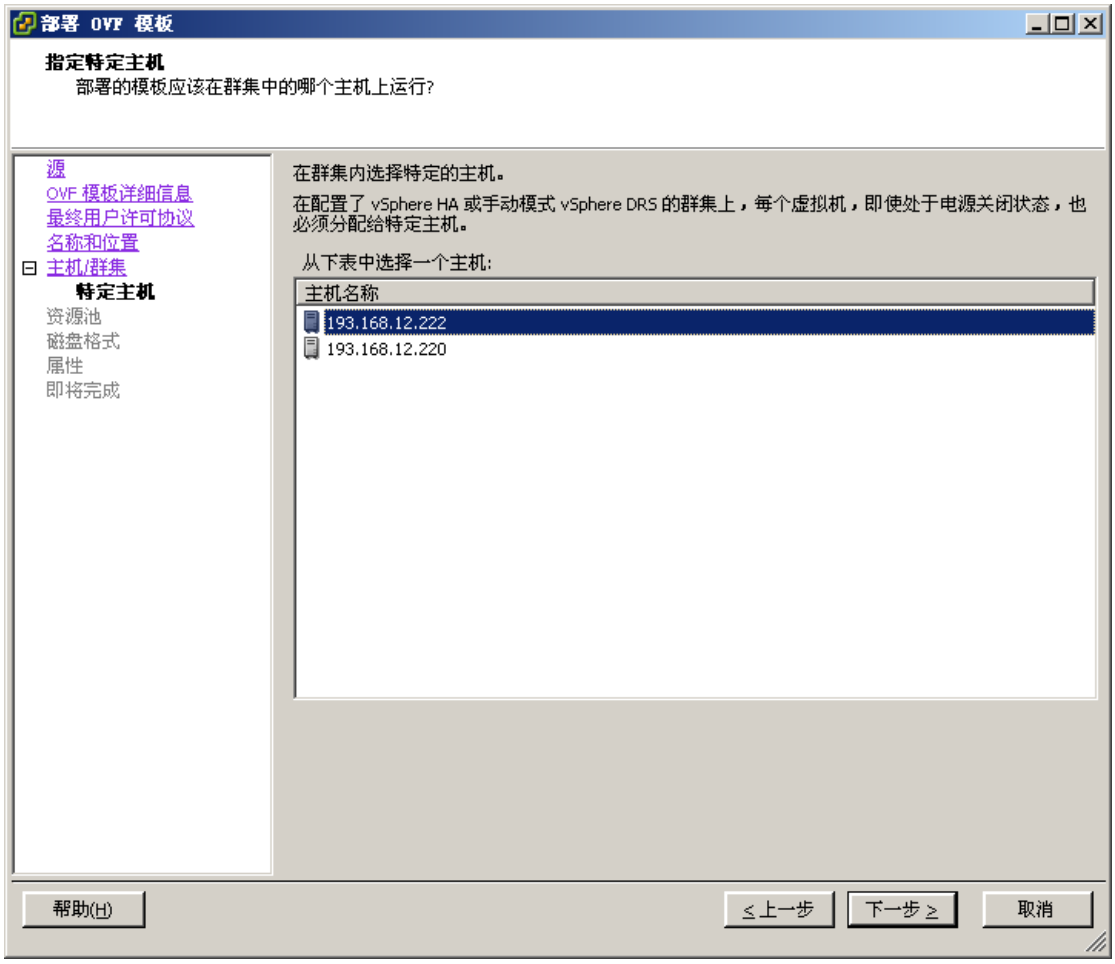
图表 3-37

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。



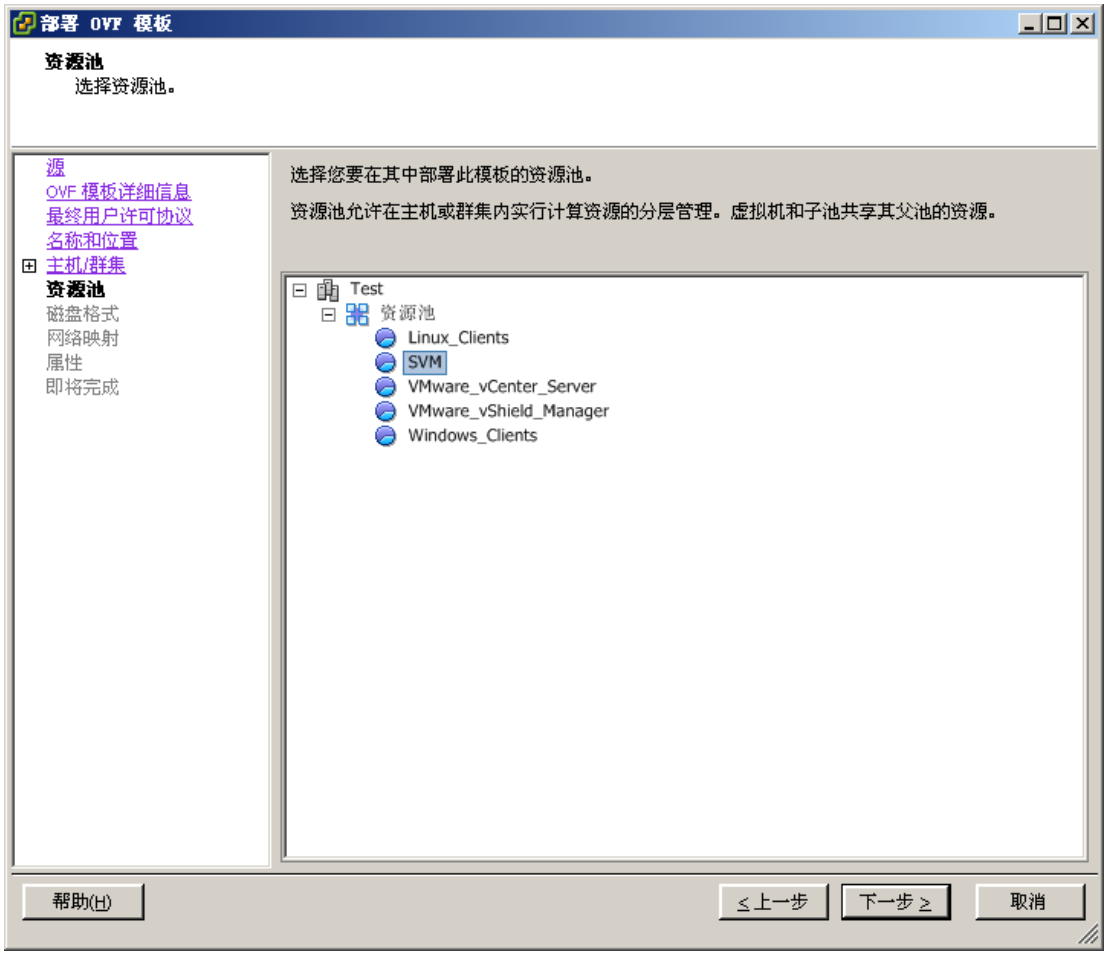
图表 3-38

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。



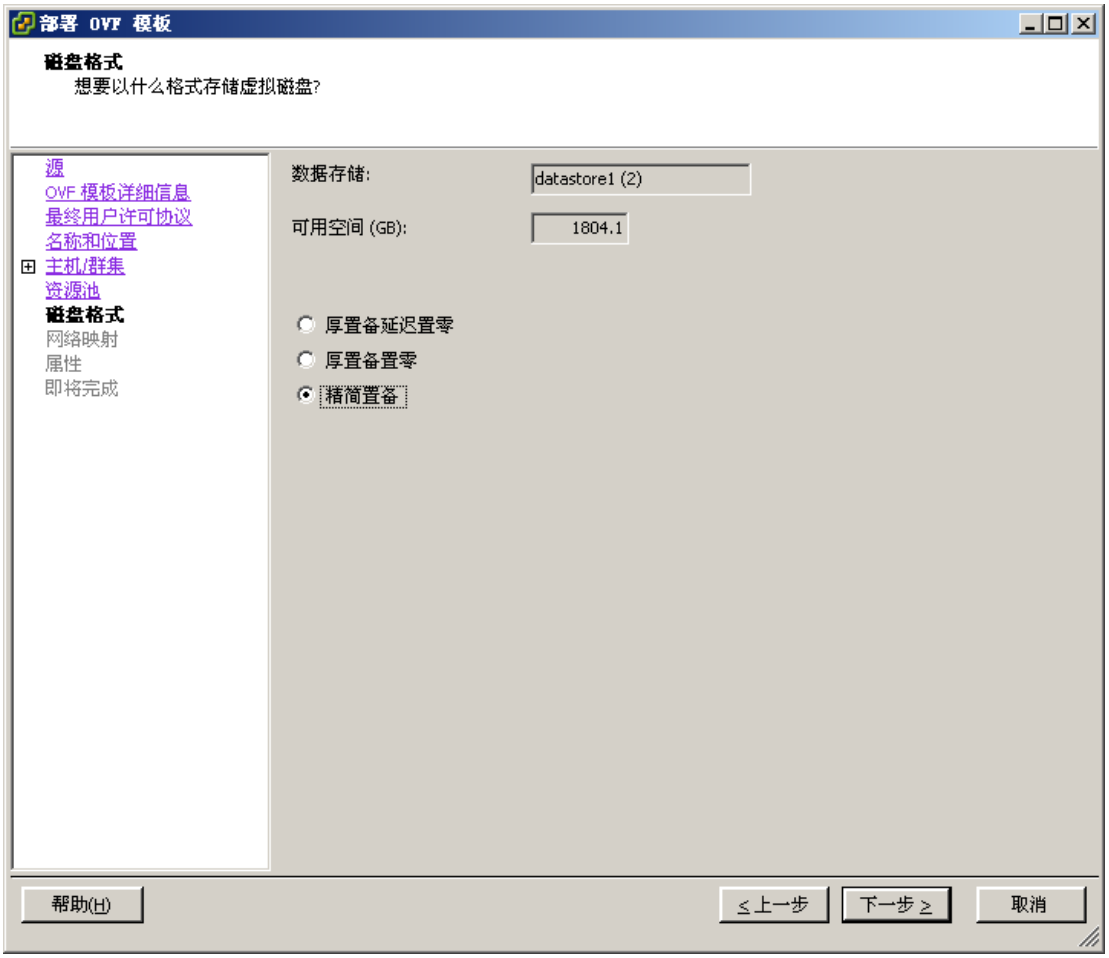
图表 3-39

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。



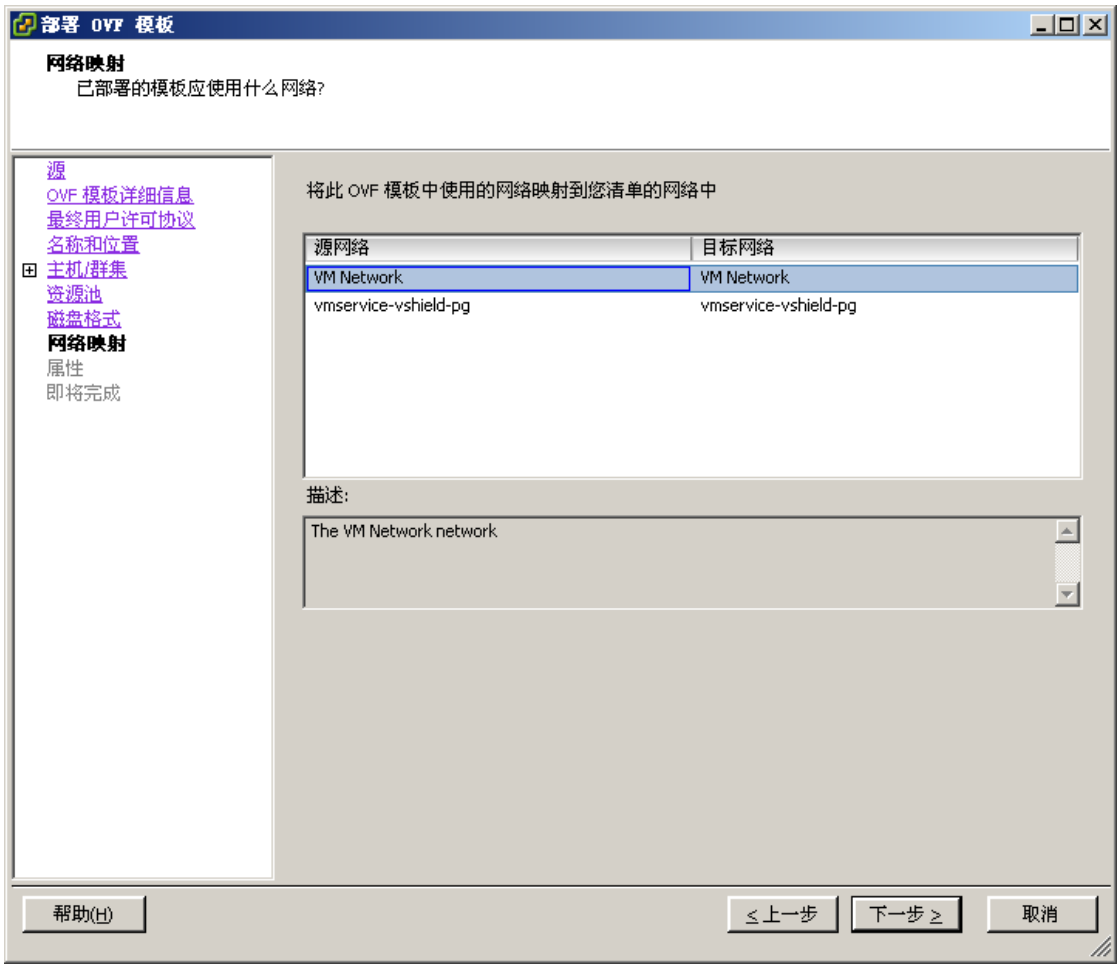
图表 3-40

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



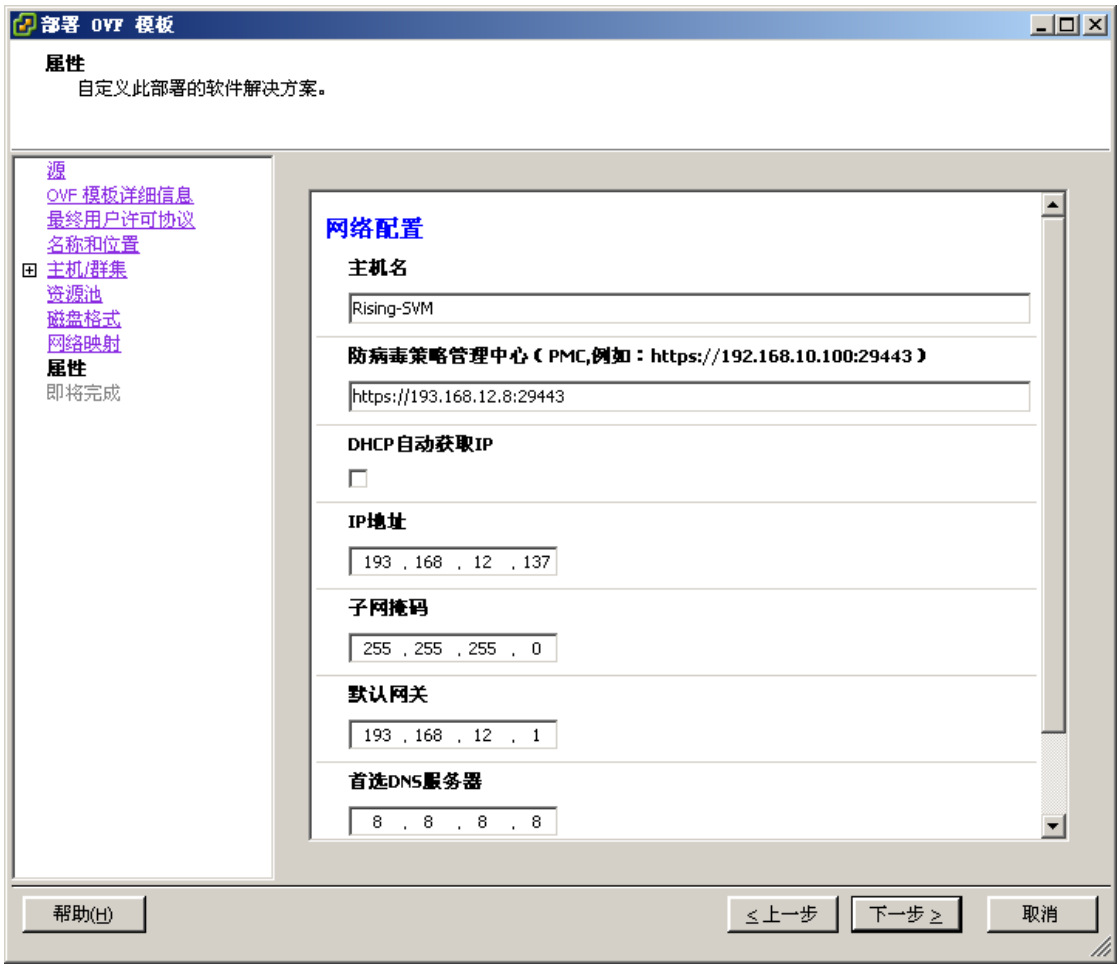
图表 3-41

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。



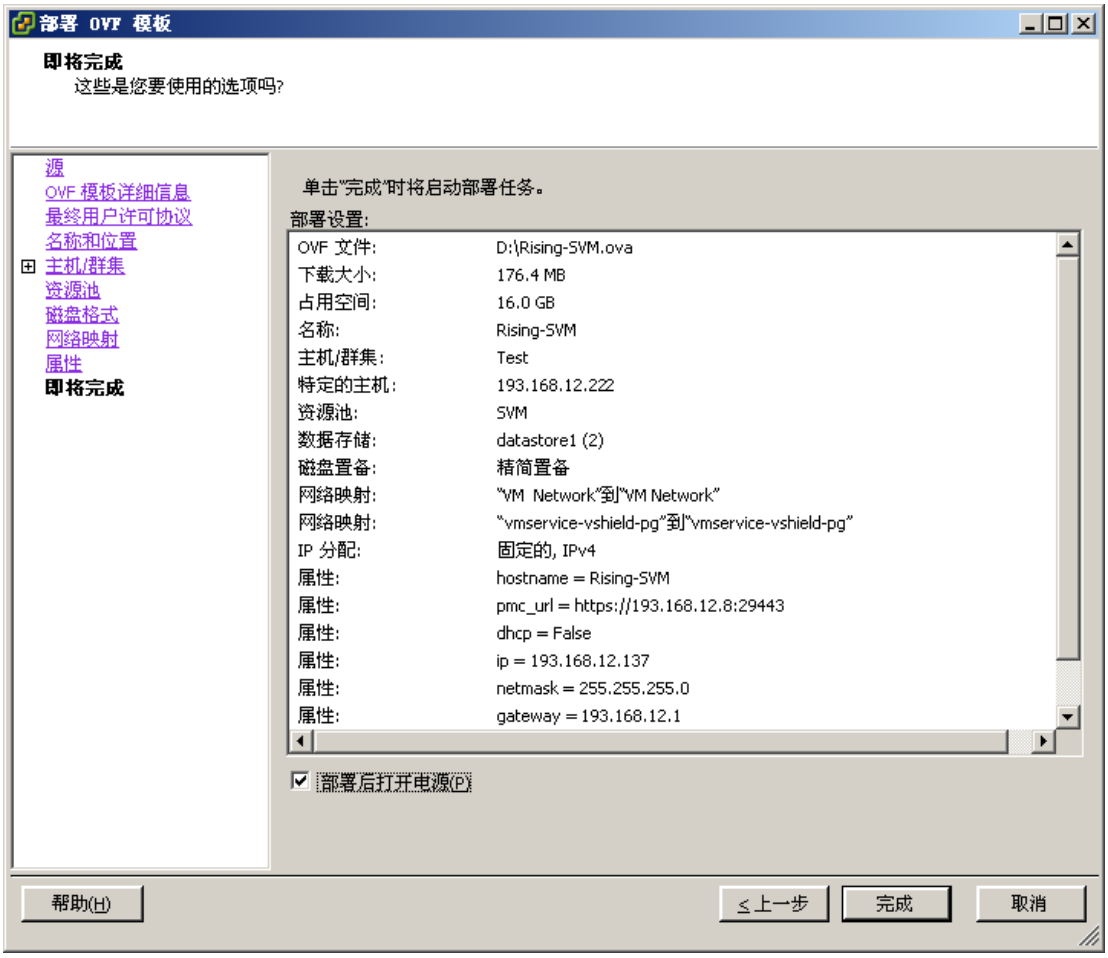
图表 3-42

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 3-43

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 3-44

提示：目前产品已经支持在管理中心部署安全虚拟设备，请参考3.2.4.2 在管理中心部署安全虚拟设备。

3.2.4.2 在管理中心部署安全虚拟设备

登录到管理中心，切换到终端，在终端列表中，勾选一台虚拟主机，使【部署安全虚拟设备】按钮激活。

图表 3-45

点击【部署安全虚拟设备】按钮，弹出部署安全虚拟设备界面，点击【选择】按钮，选择安全虚拟设备文件路径。

图表 3-46

点击【上传】按钮，即开始上传文件。

图表 3-47

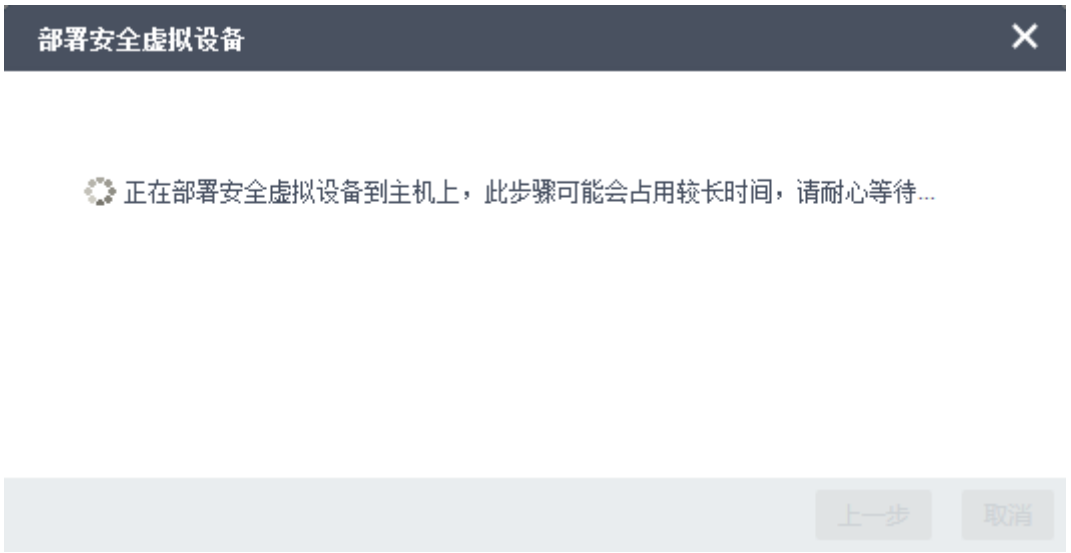
上传完成，如下图所示：

图表 3-48

点击【下一步】，弹出部署安全虚拟设备界面。

图表 3-49

填写相关配置信息，点击【下一步】，开始部署安全虚拟设备。



图表 3-50

部署完成，如下图所示：

图表 3-51

提示：安全虚拟设备激活方式，请参考本文档章节[3.3.2 激活VMware安全虚拟设备](#)。

3.2.4.3 安全虚拟设备推荐配置

安全虚拟设备 OVA 模板默认配置为 2 VCPU、2GB 内存，用户可根据需要保护的客户虚拟机数量进行自定义，从而达到最佳性能，推荐配置如下：

客户虚拟机（个数）	安全虚拟设备配置	
	VCPU（个数）	内存(GB)
<=30	2	2
>30,<=50	2	4
>50	4	8

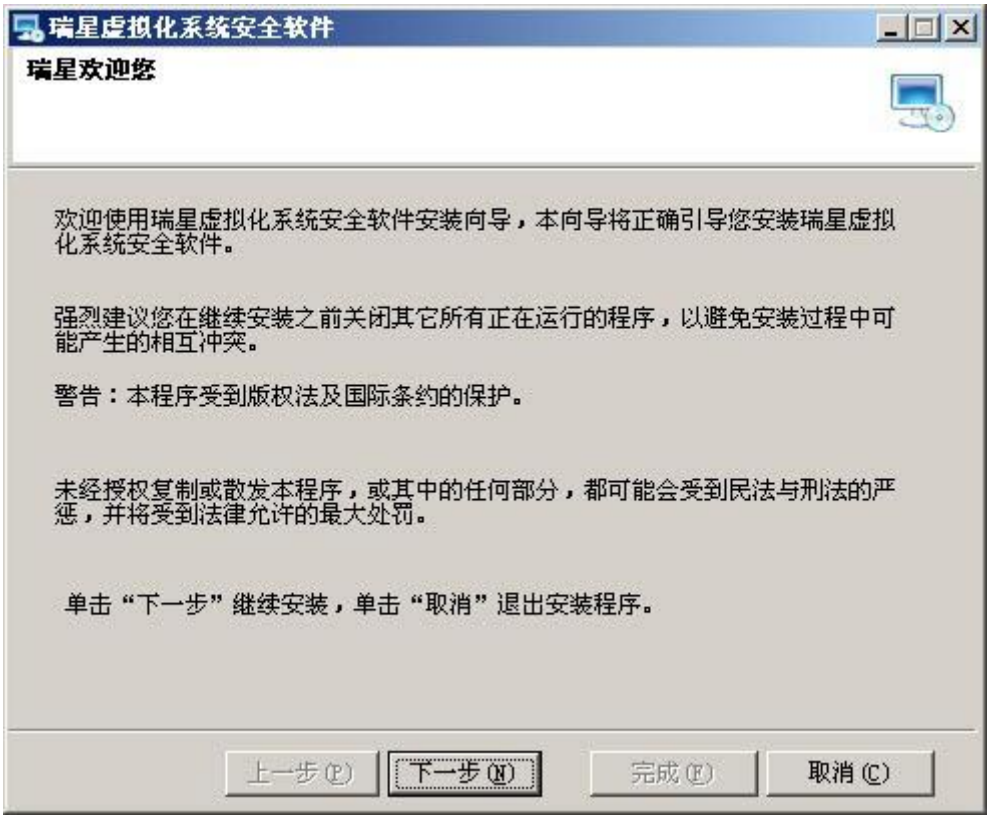
图表 3-52

3.2.4.4 RSTools

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

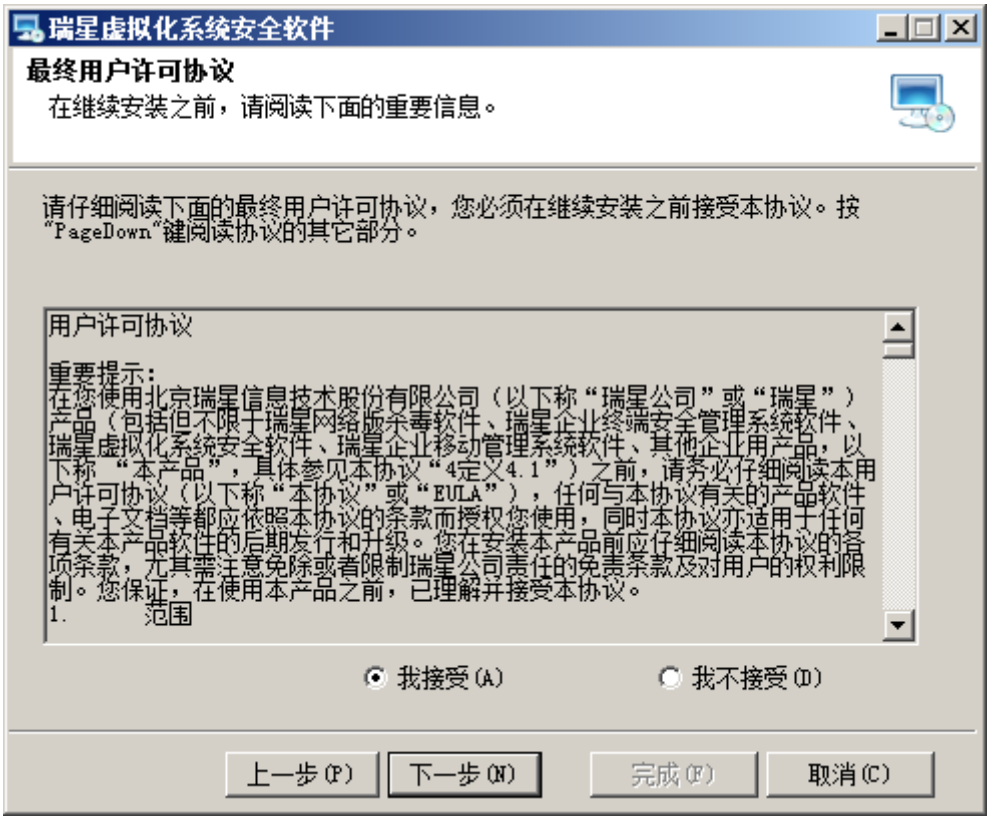
图表 3-53

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 3-54

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 3-55

第四步：在【定制安装】界面选择【RSTools】组件，点击【下一步】继续安装。

图表 3-56

第五步：在【客户端选项】界面显设定客户端参数，点击【下一步】继续安装。

图表 3-57

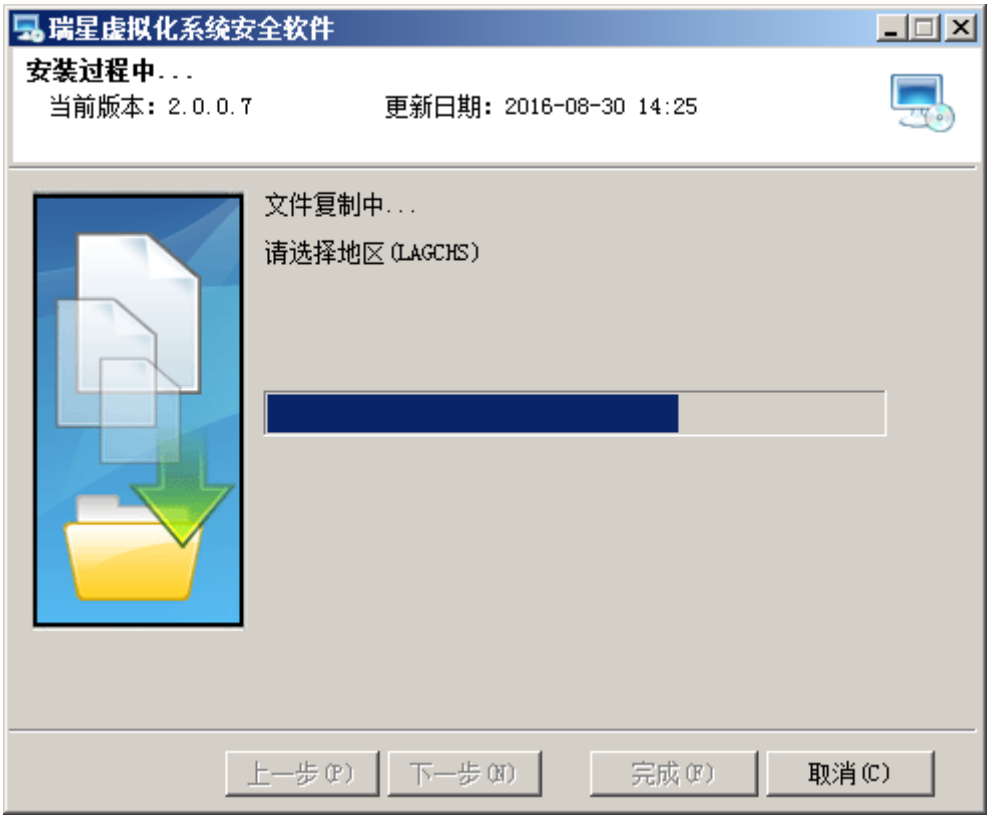
第六步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，点击【下一步】继续安装。

图表 3-58

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 3-59

第八步：显示安装过程信息。



图表 3-60

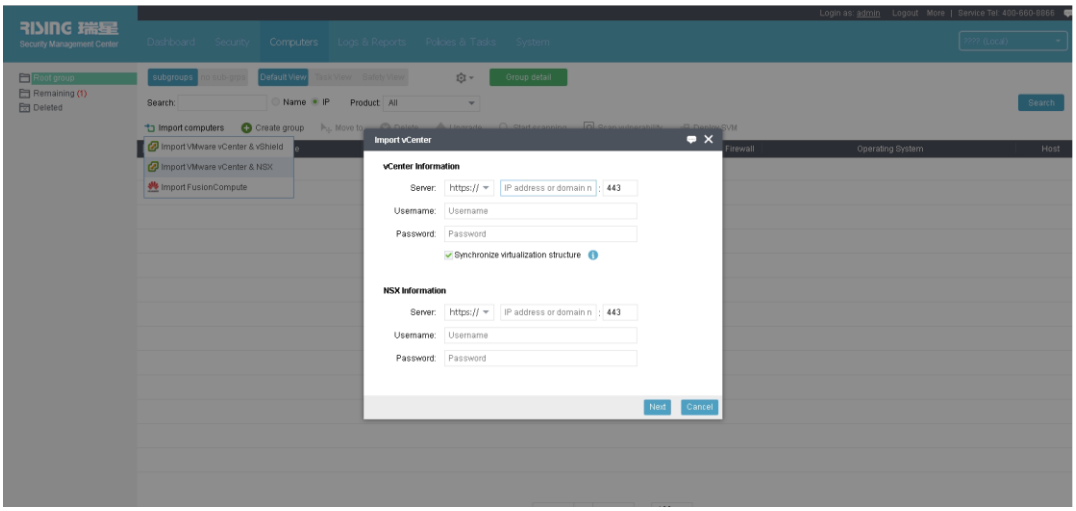
第九步：完成瑞星虚拟化系统安全软件 RSTools 安装过程。

图表 3-61

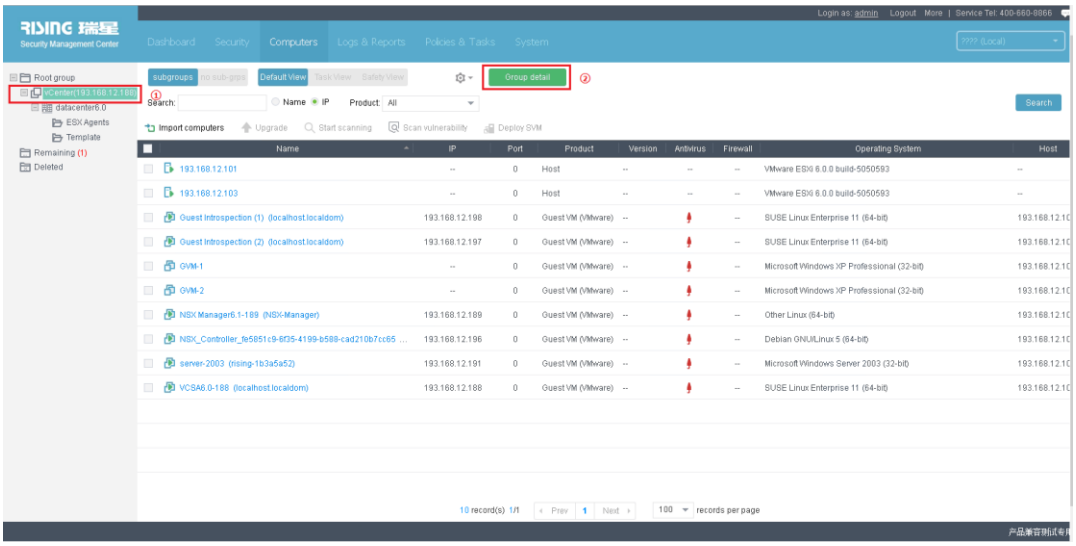
3.2.5 VMware 无代理杀毒（NSX）

3.2.5.1 安全服务虚拟机

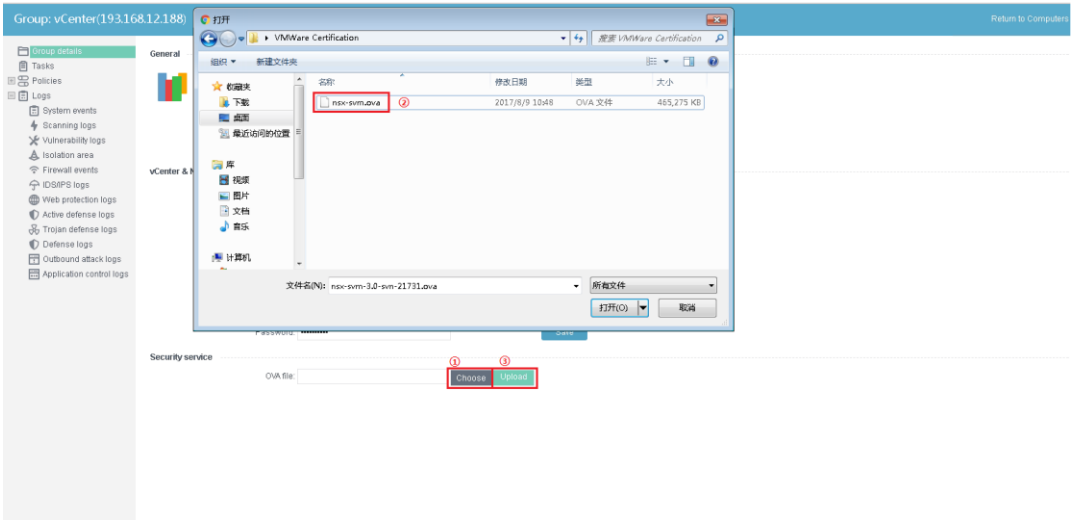
第一步：登录到管理控制台（https://IP:29443/rvsmc），在【终端管理】中选择【导入 VMware vCenter & NSX】，填写相应信息。



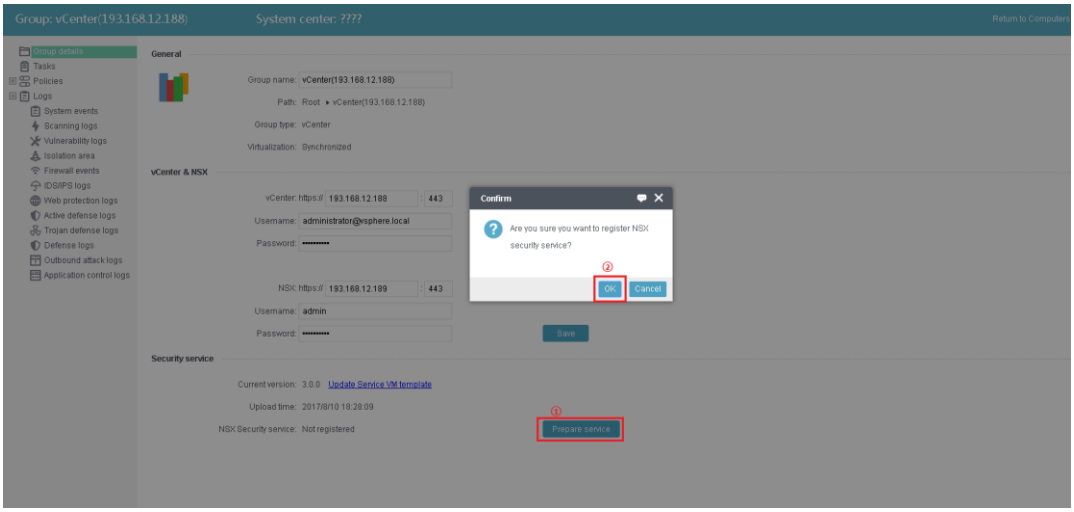
第二步：导入成功后，在左侧树上选中刚添加的 vCenter，点击【当前组信息】。



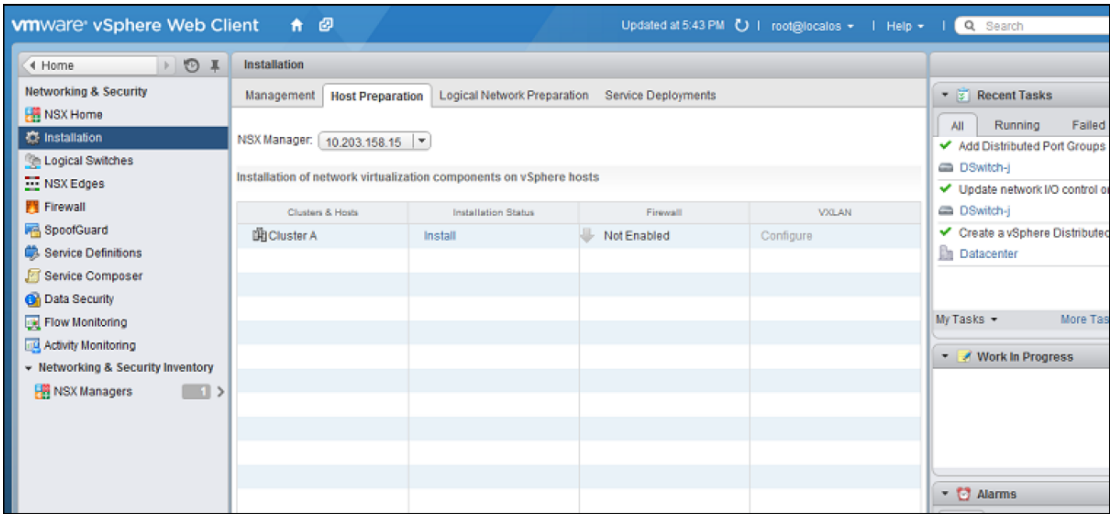
第三步：在组详情页面底部，上传 svm 对应的 ova 文件。



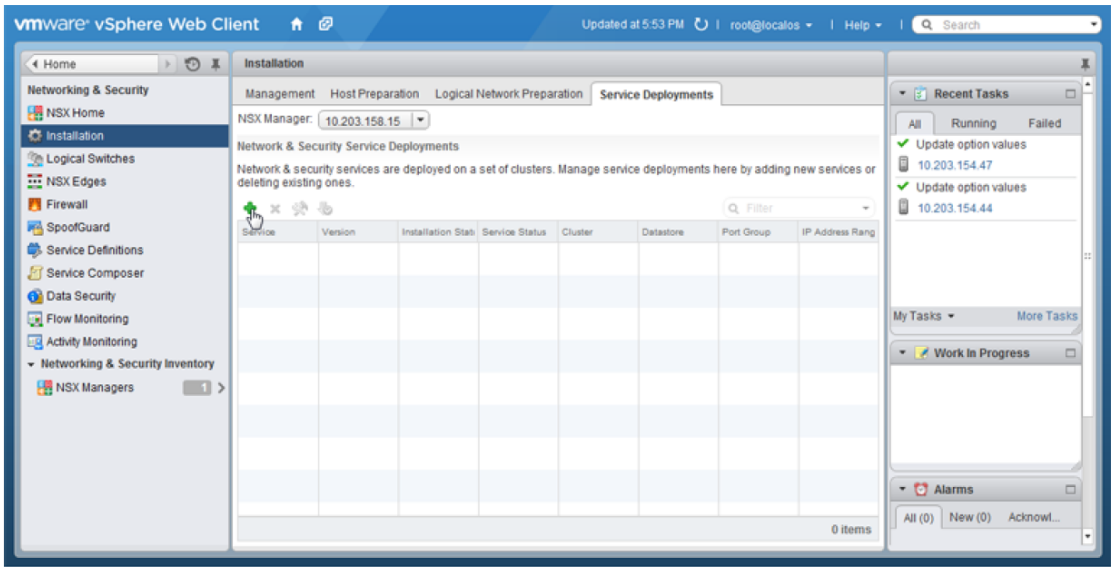
第四步：当上传完成后，会出现【准备服务】按钮。点击此按钮，向 NSX 注册瑞星安全服务 RisingCloudSec。



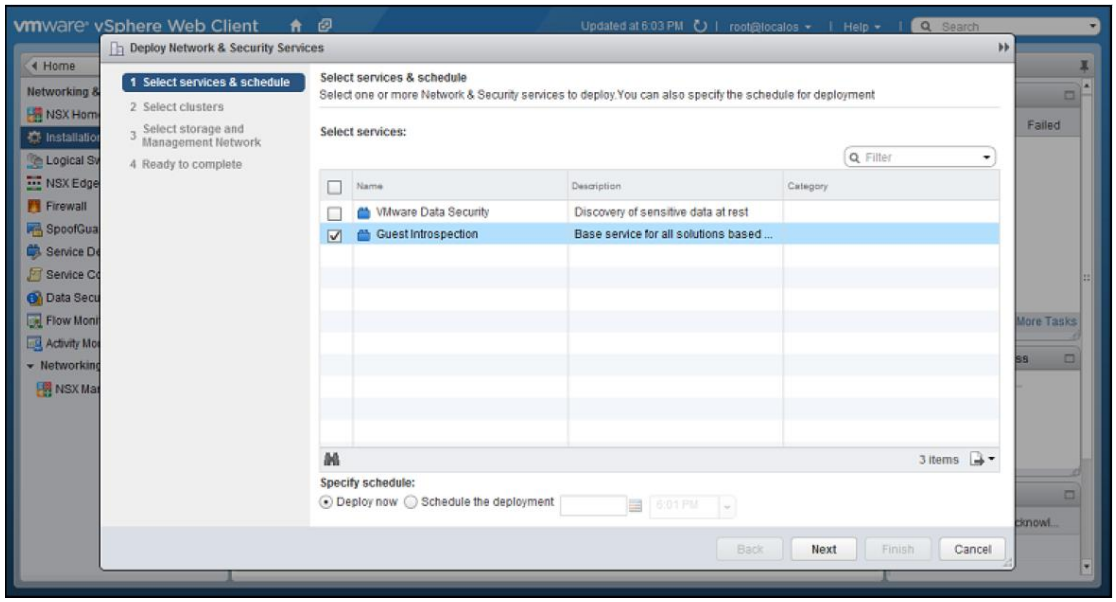
第五步：准备 ESXi。在 vSphere Web Client 中，转至主页 > 网络和安全 > 安装，在【主机准备】选项卡中，为选定的集群安装 Introspection 服务。



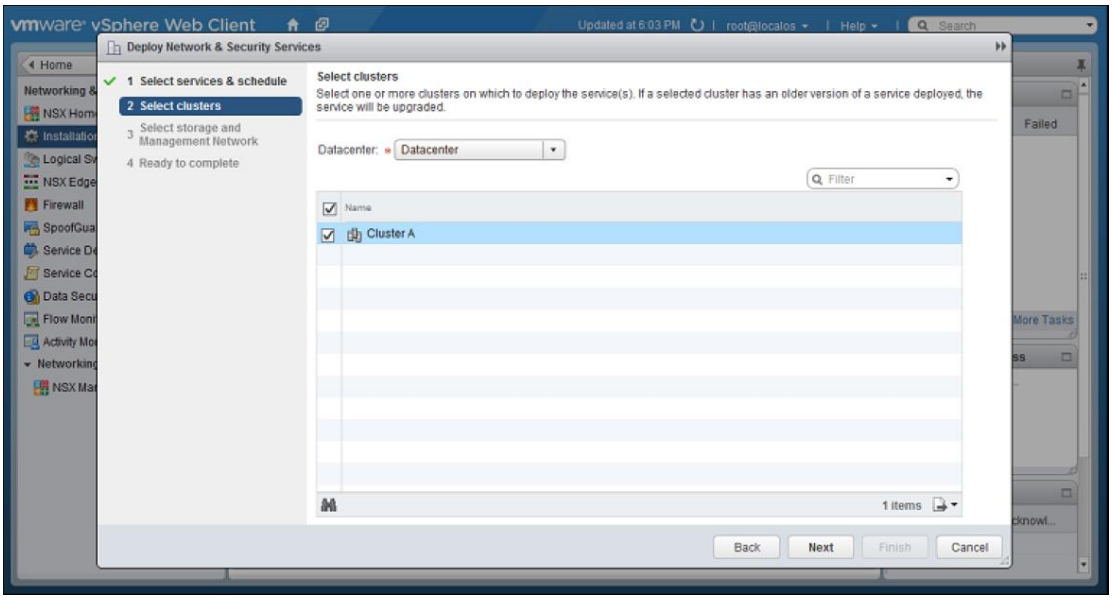
第六步：在 NSX 中部署 Guest Introspection 服务与 RisingCloudSec 服务。在 vSphere Web Client 中，切换至【服务部署】选项卡，点击【+】号。



勾选 Guest Introspection 服务。

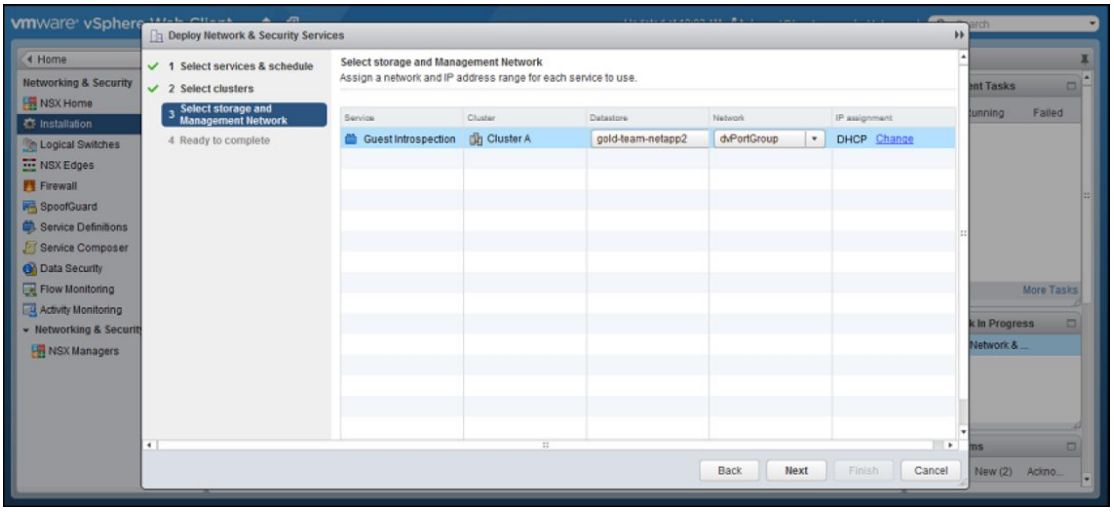


选择要保护的群集。



选择存储、网络、IP。

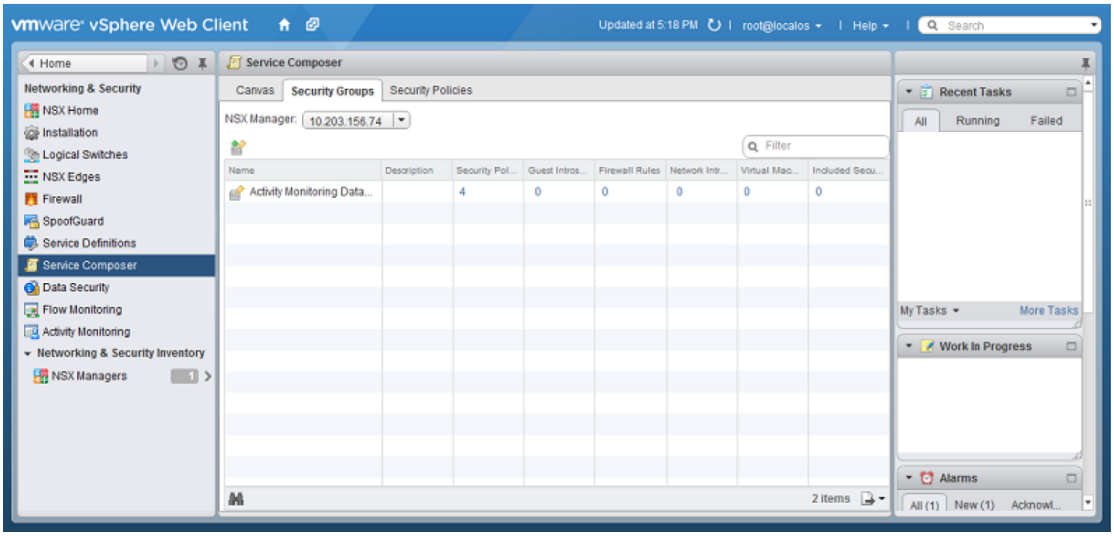
对于未配置共享存储的环境，请在各主机上分别指定本地存储，然后此页面可以选择【在主机上指定】。网络建议使用分布式端口组。IP 请指定 DHCP 或 IP Pool。



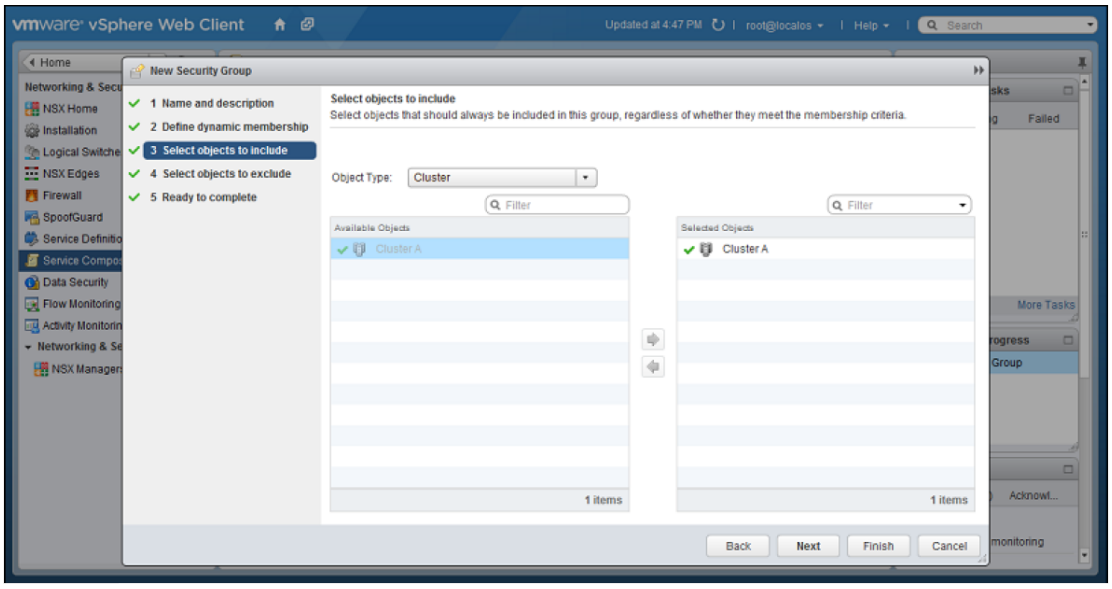
后续安装过程将需要一定时间，请耐心等待。Guest Introspection 服务部署完成后，请使用相同的方法继续部署 RisingCloudSec 服务。

3.2.5.2 创建安全组与指定安全策略

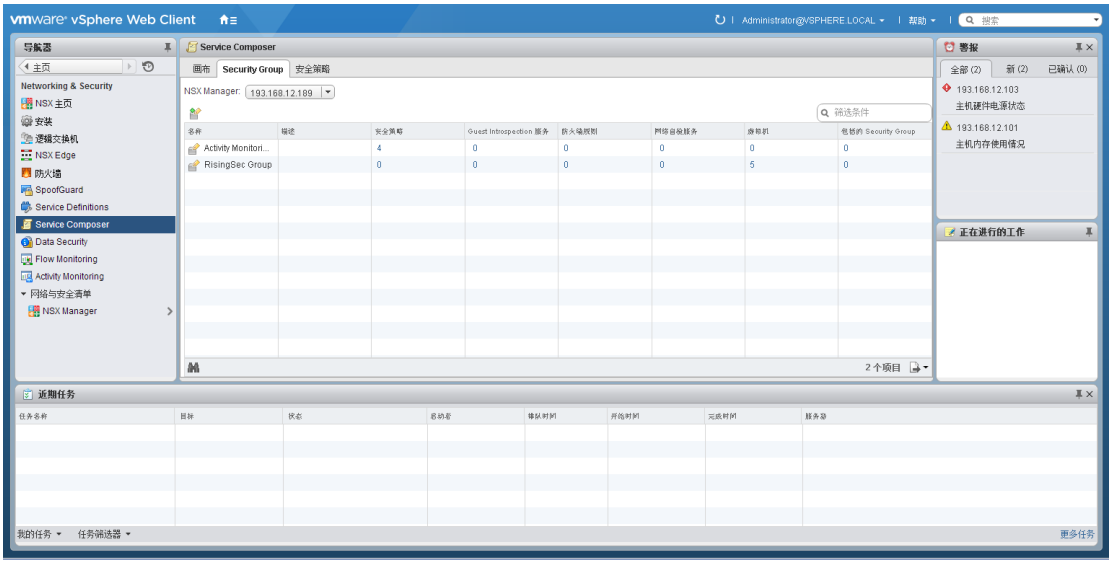
第一步：创建安全组。在 vSphere Web Client 中，转到主页 > 网络和安全 > 服务编排，添加安全组。



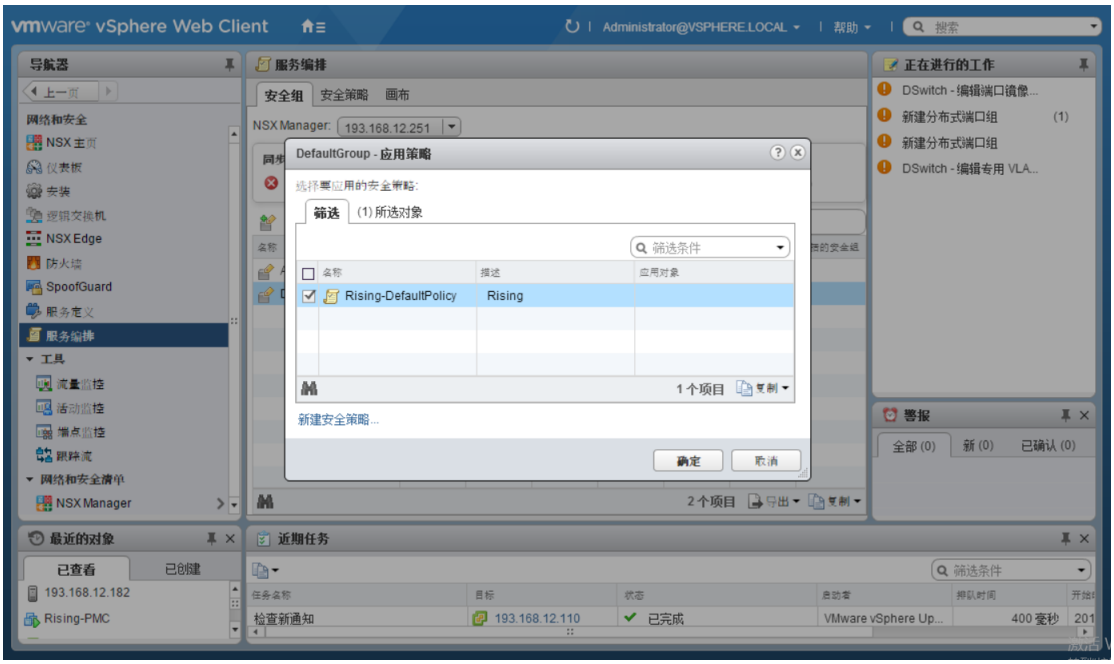
为此安全组定义成员，可以设置动态过滤条件或直接选定范围。



完成后可以在列表中看到新创建的安全组。



第二步：为创建好的安全组指定安全策略。选中刚创建的安全组，点击【应用策略】，在列表中勾选【Rising-DefaultPolicy】，确定。



3.2.5.3 RSTools

与 vShield 环境下部署 RSTools 相同，参见 3.2.4.4 节。

3.2.6 HUAWEI 无代理杀毒

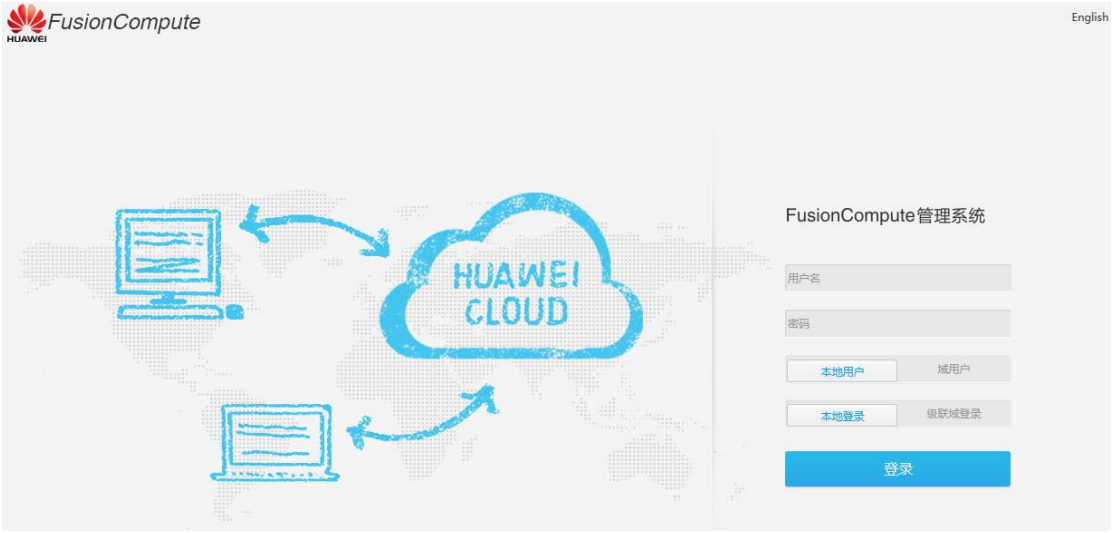
3.2.6.1 安全虚拟设备

首先将载有 SVM 模板的光盘放入光驱，SVM 模板文件是一个 OVA 模板，名称为 Rising-SVM.ova。

图表 3-62

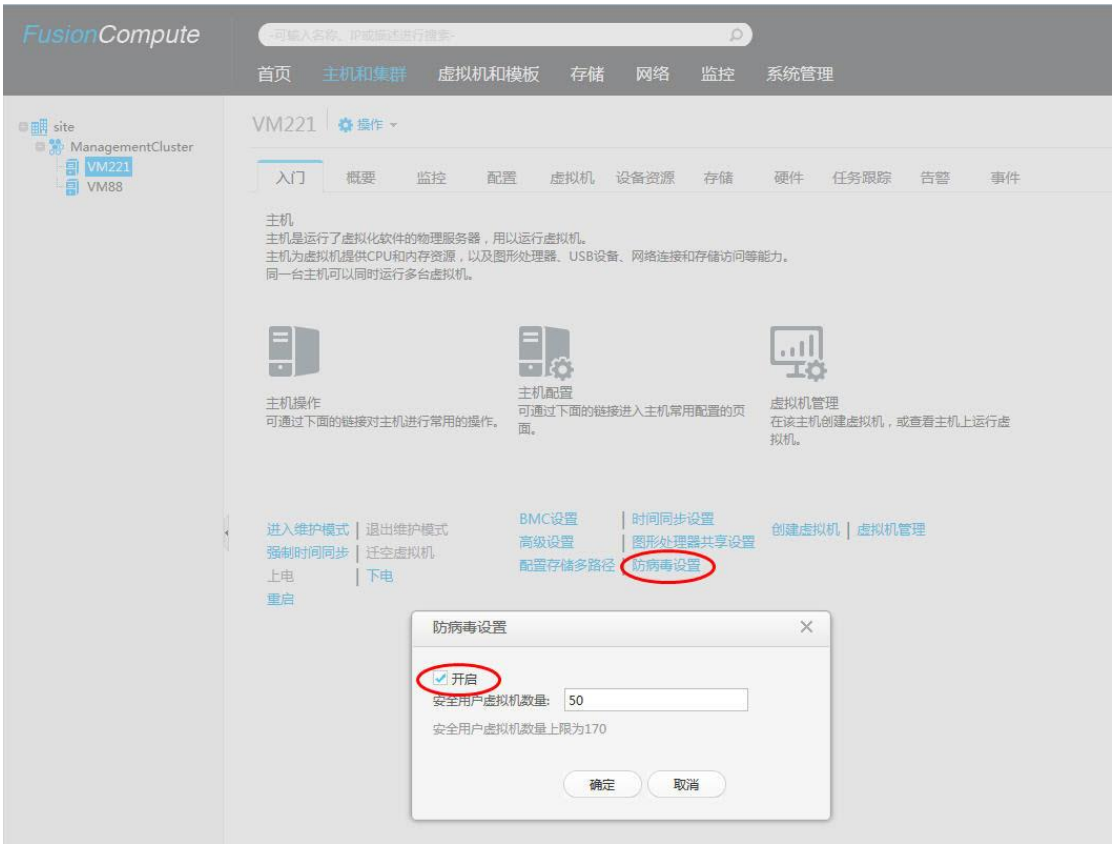
提示：SVM，安全虚拟设备，与虚拟化厂商合作开发，通过专用技术为部署在同一物理服务器上的其他Windows虚拟机提供不需要安装杀毒软件的，高效率的无代理防毒服务，可确保在最小的资源损耗下实现对所有Windows虚拟机的防病毒保护功能。

打开网页浏览器，以 admin 身份登录华为虚拟化平台 VRM 控制节点。



图表 3-63

登录后首先要打开主机（CNA 服务器）的【防病毒保护】功能，具体为在“主机和集群”页面下，选择某个主机，点击“入门”->“防病毒配置”部分，选择开启防病毒，并填写希望在此台服务器上保护的“安全用户虚拟机”（GVM）数量，确认；（注：开启此功能可能需要主机进行重启）



图表 3-64

当“防病毒配置”开启后，就可以继续导入模板了。选择“虚拟机和模板”->“导入虚拟机”。

图表 3-65

在下一个页面中选择“导入源”为“从本地导入”，点击“下一步”

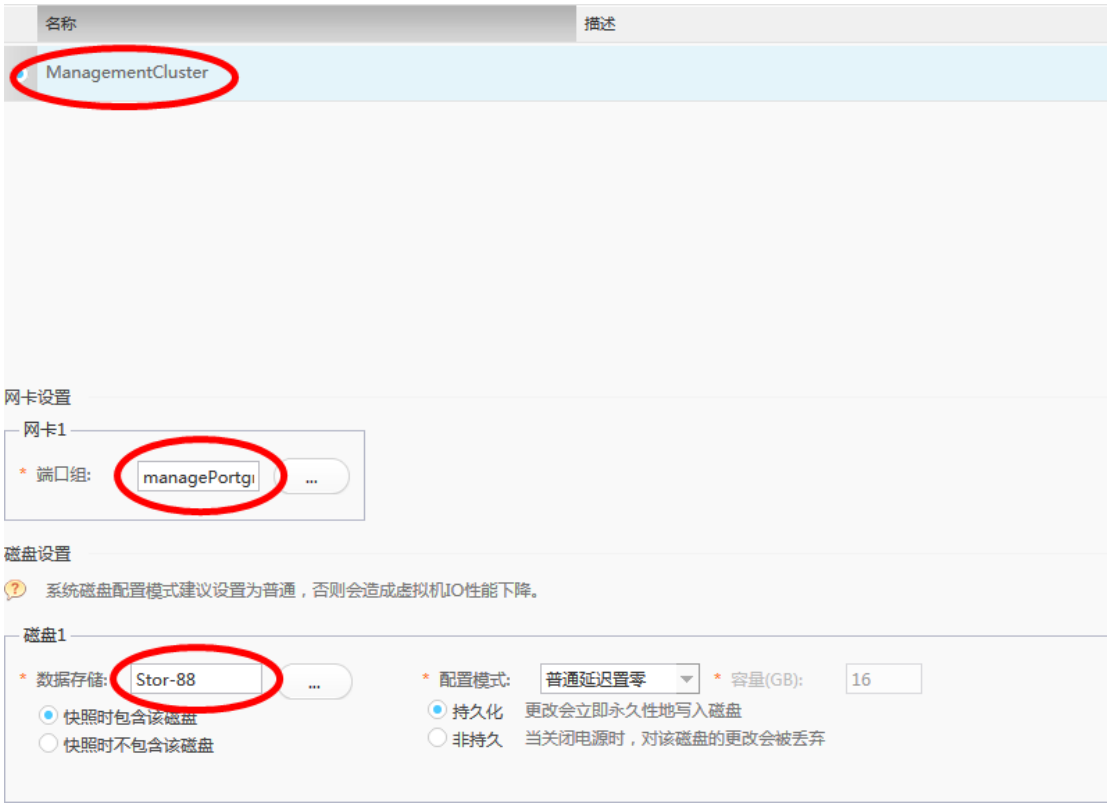
图表 3-66

在下一个页面“模板文件”栏“浏览”选择光盘上的 SVM 模板文件：Rising-SVM.ova，点击“下一步”（注：此步骤可能需要浏览器安装并运行 Java 插件以正常显示浏览框）。

图表 3-67

在下一个页面，选择 SVM 虚拟机所在集群和网卡及磁盘配置，选择某个集群后，在“网卡设置”处，选择网卡和端口组，SVM 只需要一块虚拟网卡，此处选择的网卡及端口组应能够与瑞星安全虚拟化软件中的 PMC 控制台所配置的网卡进行正常通讯。之后设置虚拟机磁盘，SVM 需要 2 块虚拟磁盘，第一块容量为 1GB，第二块容量为 15GB，所选择的数据存

储应至少有 16GB 可用空间来分配给 SVM，选择好后点击“下一步”

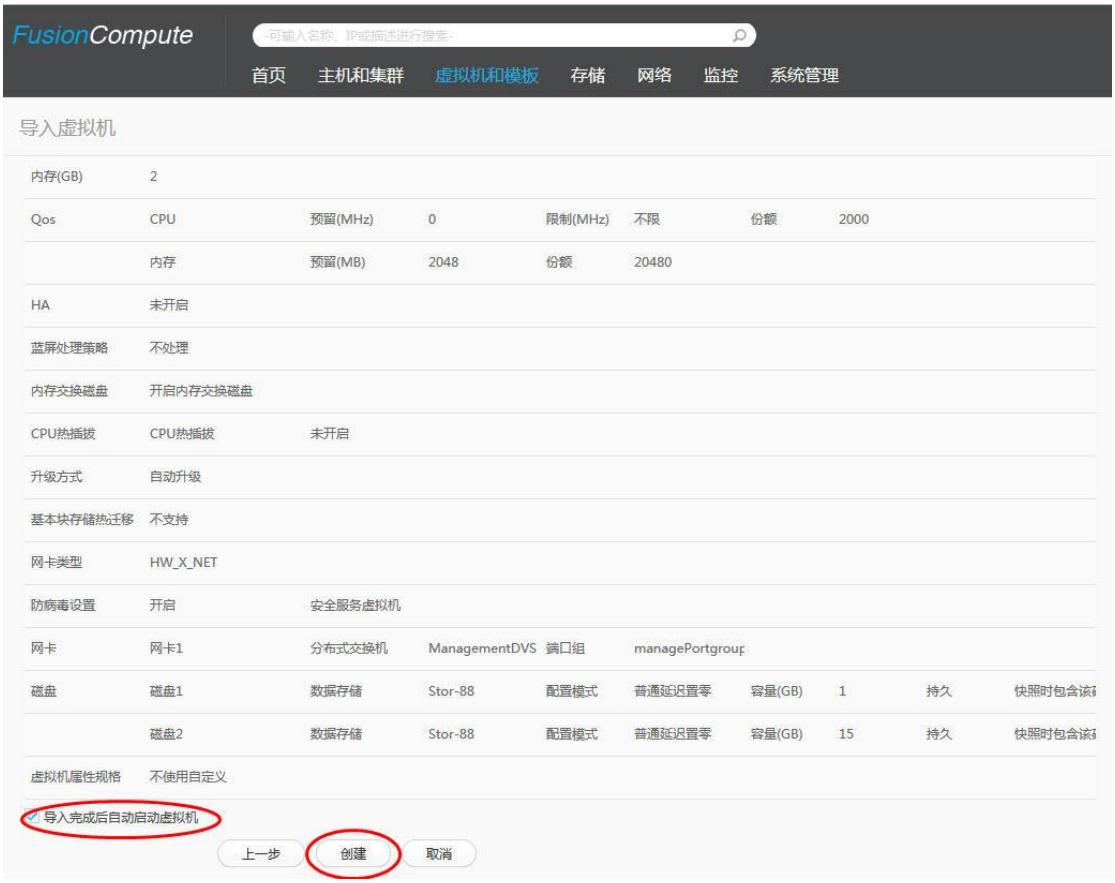


图表 3-68

在下一个页面中，填写“虚拟机名”（比如 Rising-SVM），打开“高级设置”，“开启”防病毒设置，并选择“安全服务虚拟机”，之后点击“下一步”

图表 3-69

在下一个页面勾选“导入完成自动启动虚拟机”，点击“创建”

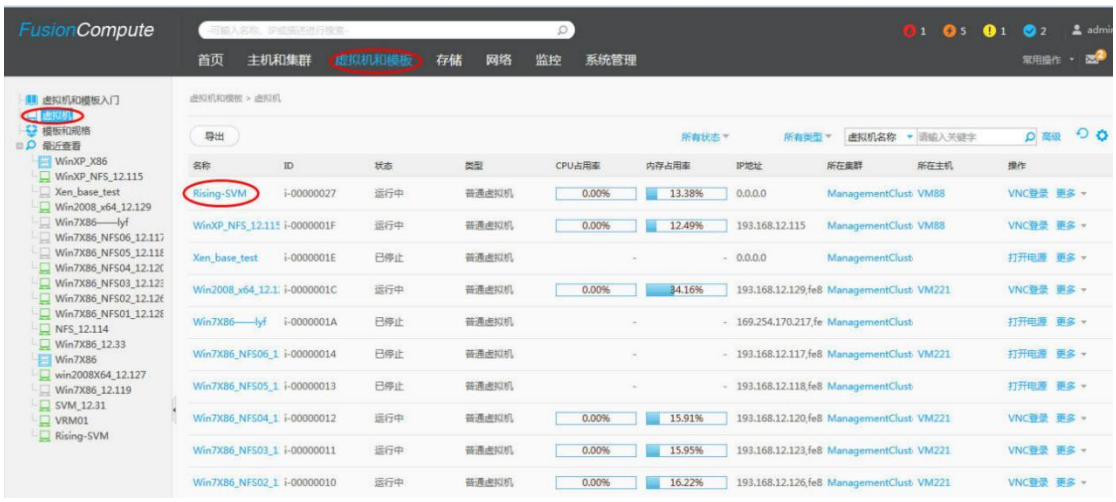


图表 3-70

之后，耐心等待 SVM 虚拟机创建成功，根据服务器配置不同，此过程可持续几分钟至十几分钟。创建成功后，点击“确定”。

图表 3-71

之后再次点击页面上的“虚拟机和模板”->“虚拟机”，在右列上方选择刚刚创建的 SVM



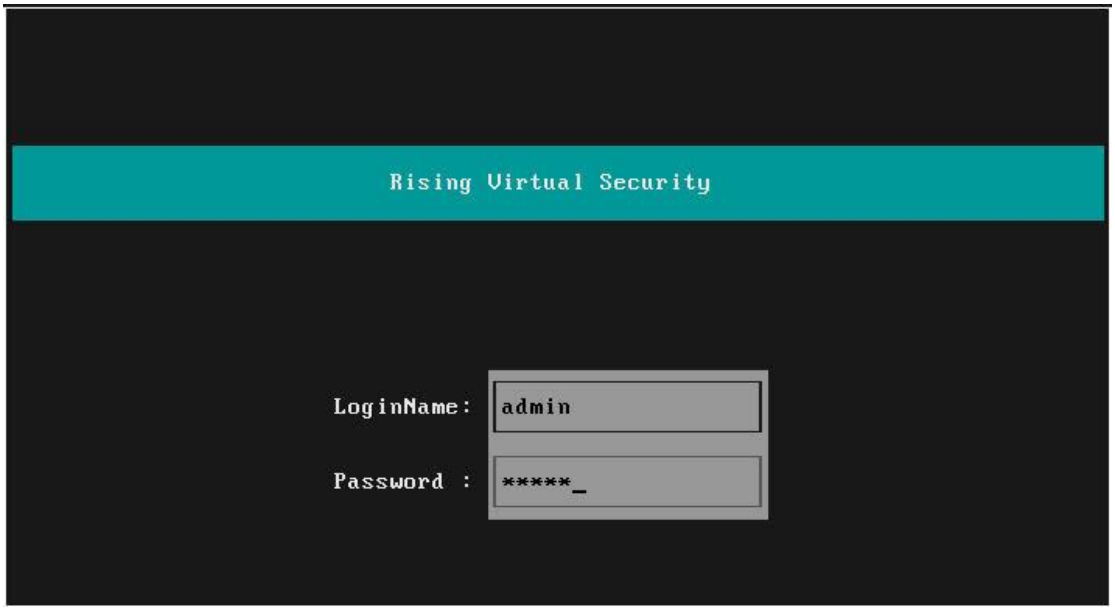
图表 3-72

点击图中“操作”之后，选择“VNC”登录，选择“noVNC”

图表 3-73

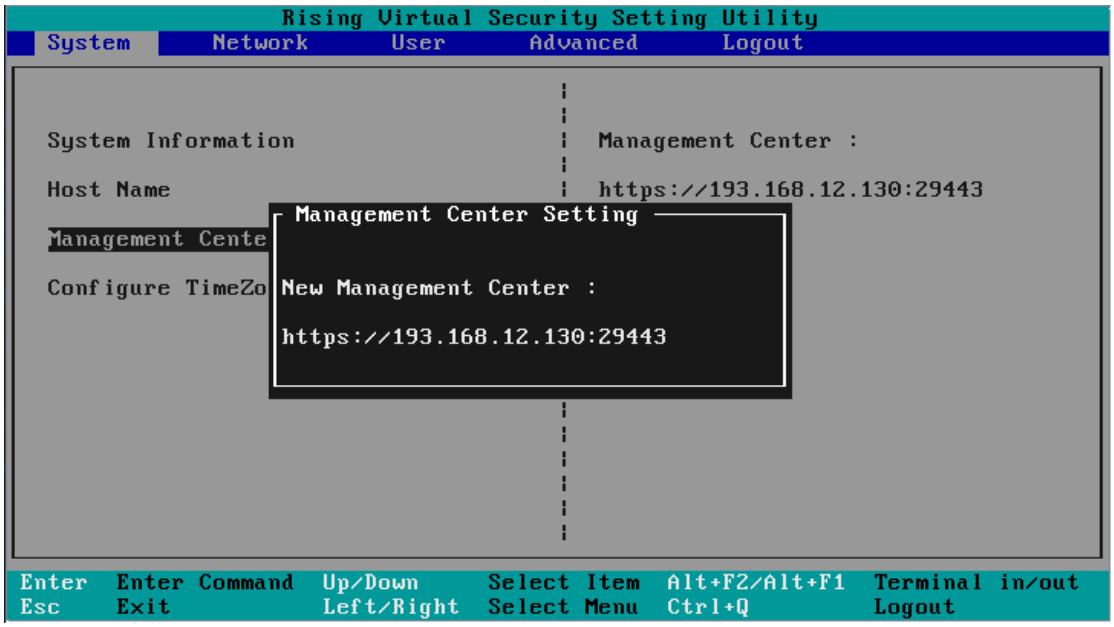
图表 3-74

在弹出的 VNC 控制台中分别在“LoginName”和“Password”均输入 admin，回车后登录 SVM 虚拟机控制界面



图表 3-75

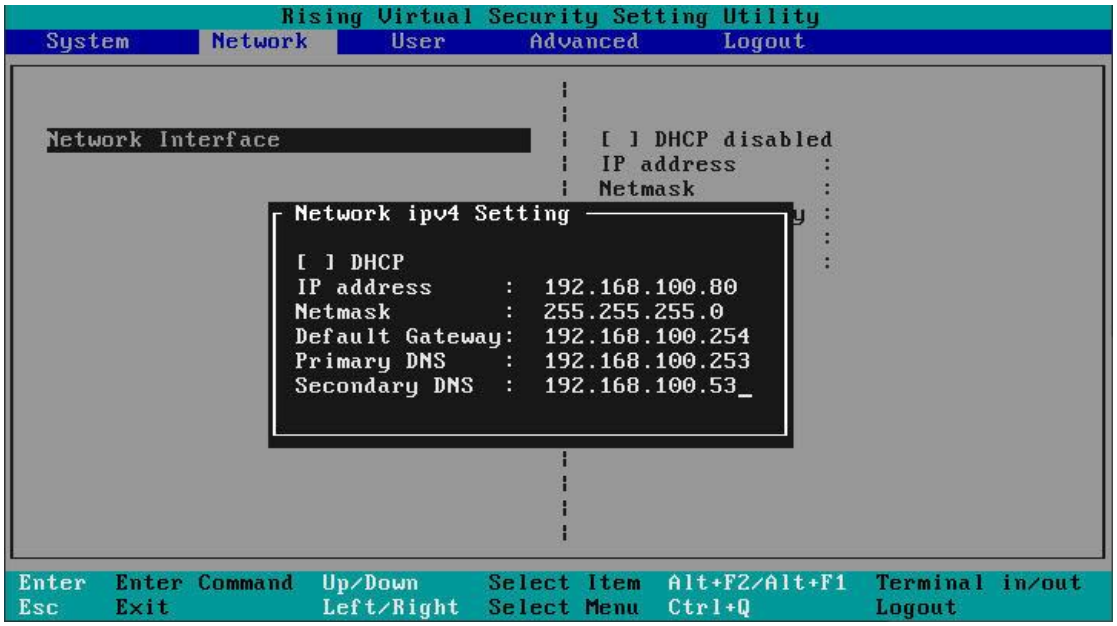
登录 SVM 控制界面后，用方向键“下”将光标选择到“Management Center”处，点击回车，在弹出的“Management Center Setting”窗口输入瑞星安全虚拟化软件 PMC 控制台的地址及端口，比如：https://193.168.12.130:29443，按回车。注：SVM 和 PMC 通过 https 来传递控制信息，此处一定要填为 https。



图表 3-76

按方向键“右”将光标调到“Network”处，点击回车，选择“Network Interface”在弹出的“Network ipv4 Setting”窗口中填入 SVM 的 ip，子网掩码，默认网关，DNS 等项目，填完其中每个项目后，用方向键“下”将光标切换到下一个项目，当需要的项目全部填写后，按回车。

注：要保证 SVM 所配地址与 PMC 控制台可正常通讯。



图表 3-77

至此我们已经完成了 SVM 的部署，但 SVM 若要正常使用，还需要从 PMC 导入并分配授权，分配授权后，SVM 就可以正常工作了。

3.2.6.2 安全虚拟设备推荐配置

安全虚拟设备 OVA 模板默认配置为 2 VCPU、2GB 内存，用户可根据需要保护的客户虚拟机数量进行自定义，从而达到最佳性能，推荐配置如下：

客户虚拟机（个数）	安全虚拟设备配置	
	VCPU（个数）	内存(GB)
<=30	2	2
>30,<=50	2	4
>50	4	8

图表 3-78

注意，HUAWEI安全虚拟设备（SVM）内存大小调整后，需要将“内存预留”调整为完全预留，否则，SVM不能正常工作。

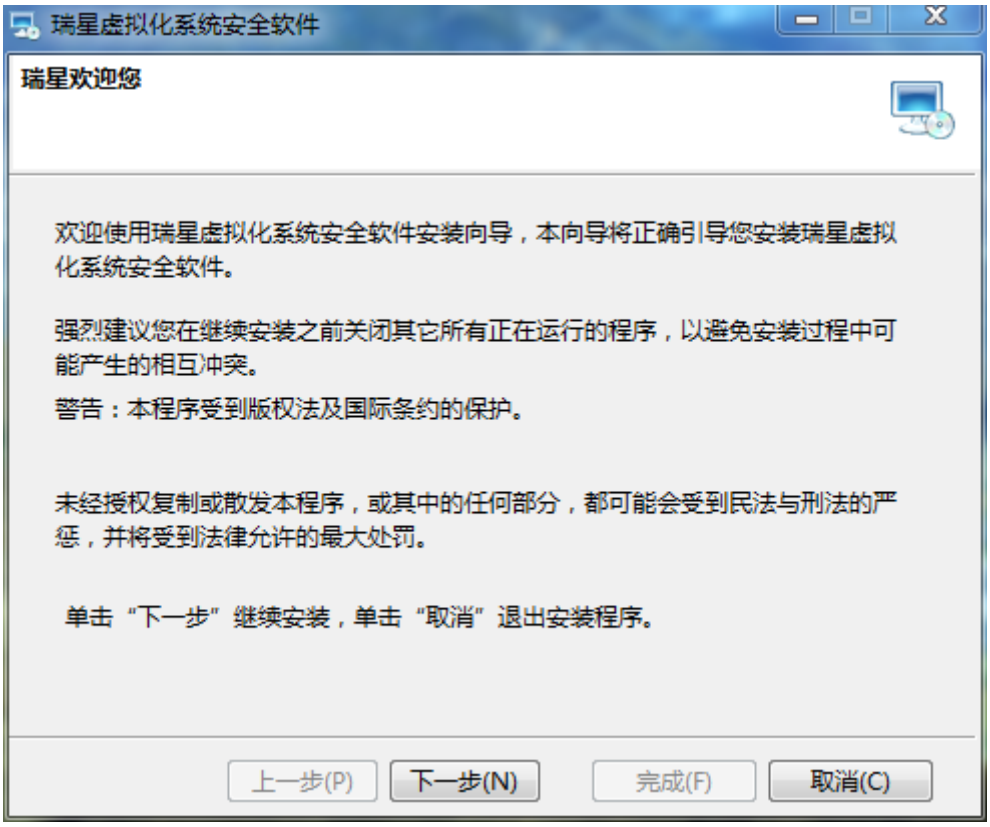
3.2.6.3 RSTools

具体操作方法请参考本文档章节 3.2.4.4RSTools。

3.2.7 安全防护终端

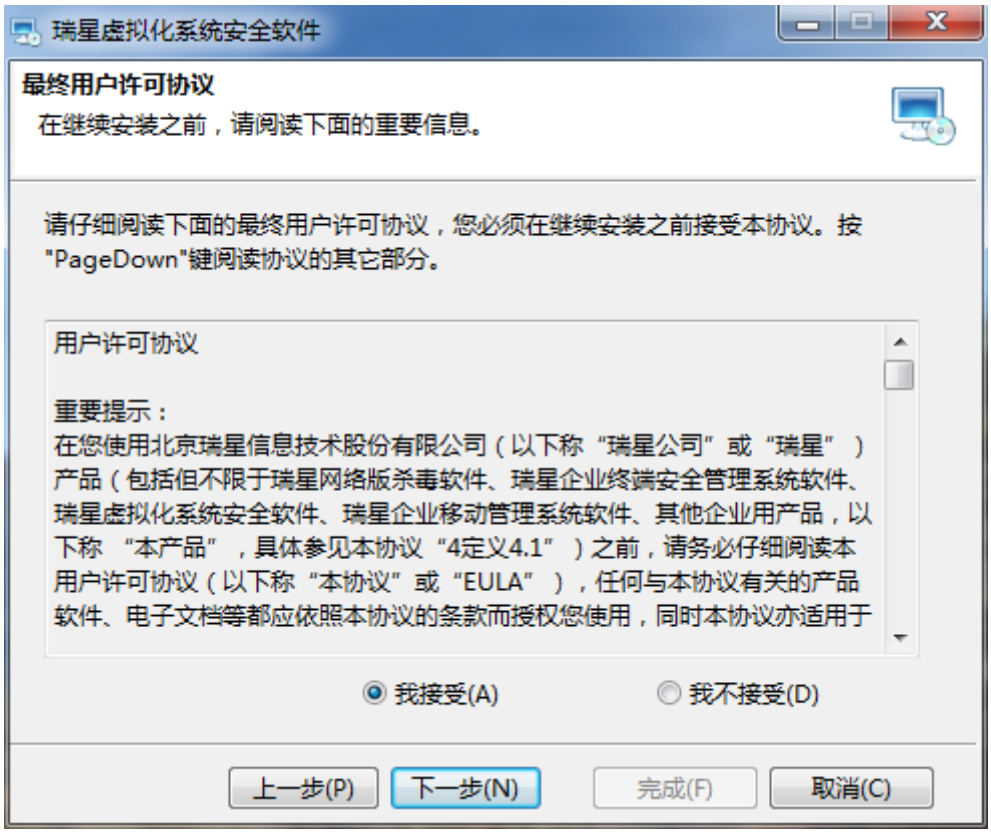
第一步：将瑞星虚拟化系统安全软件光盘放入光驱内进入到安全防护终端安装包目录下，运行 RVS.exe 安装程序。

第二步：进入安装程序欢迎界面，单击【下一步】继续安装，还可以通过【取消】按钮退出安装过程。



图表 3-79

第三步：弹出【最终用户许可协议】窗口，请仔细阅读软件许可协议。如果接受，请选择【我接受】，单击【下一步】继续安装；如不接受该协议，选择【我不接受】退出安装程序。

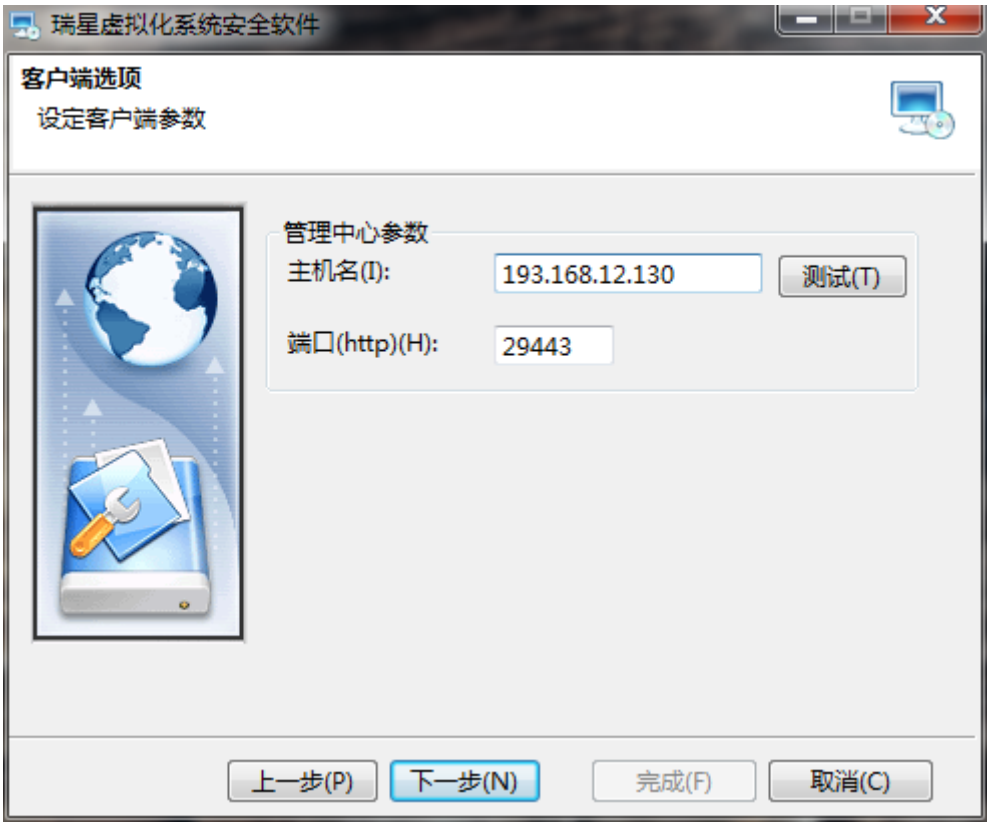


图表 3-80

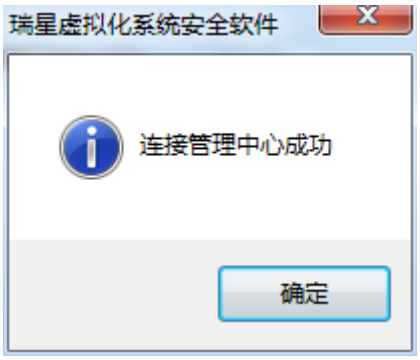
第四步：进入【定制安装】界面，选择需要安装的【安全终端】组件，单击【下一步】继续安装。

图表 3-81

第五步：进入【客户端选项】界面，指定管理中心 IP 地址，单击【测试】按钮可以测试客户端与管理中心之间的连通性，单击【下一步】继续安装。

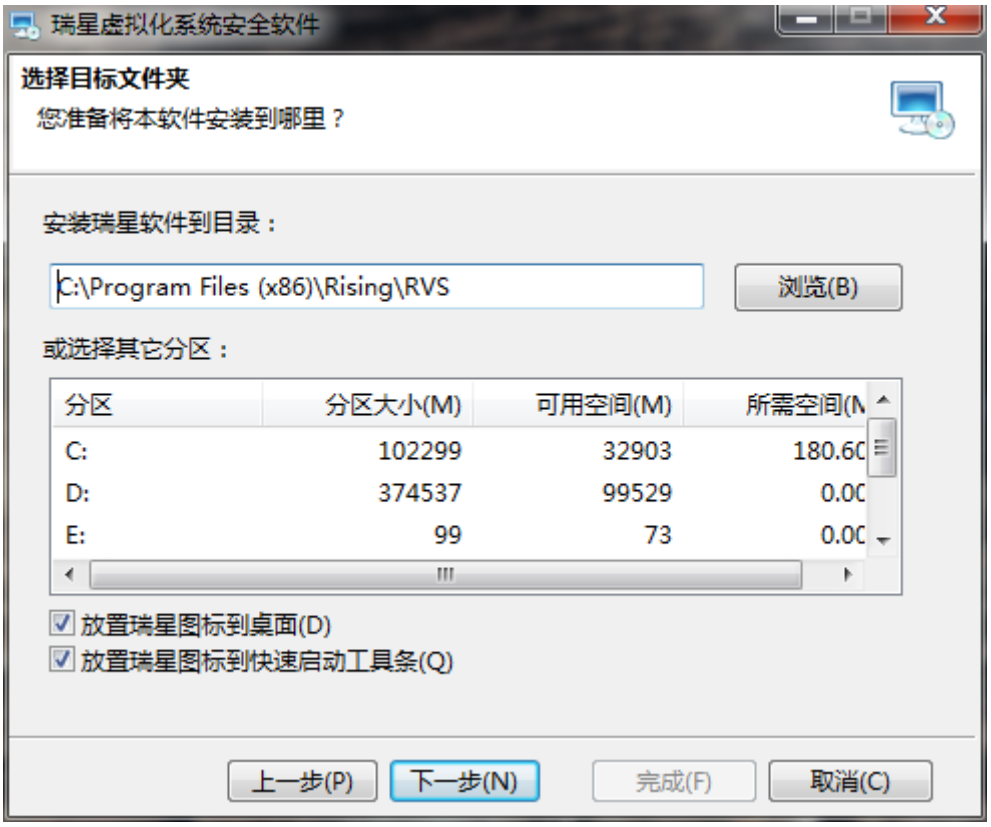


图表 3-82



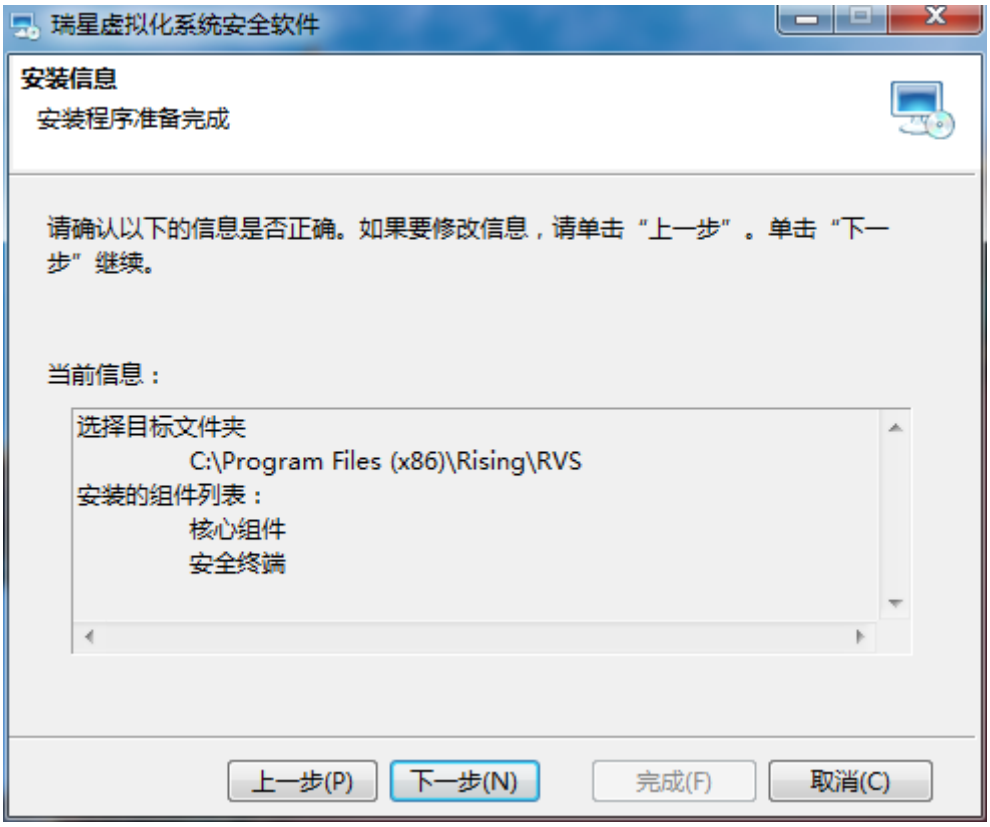
图表 3-83

第六步：在【选择目标文件夹】界面中，选择安装瑞星虚拟化系统安全软件的目标文件夹，勾选【放置瑞星图标到桌面】和【放置瑞星图标到快速启动工具栏】，单击【下一步】继续安装。



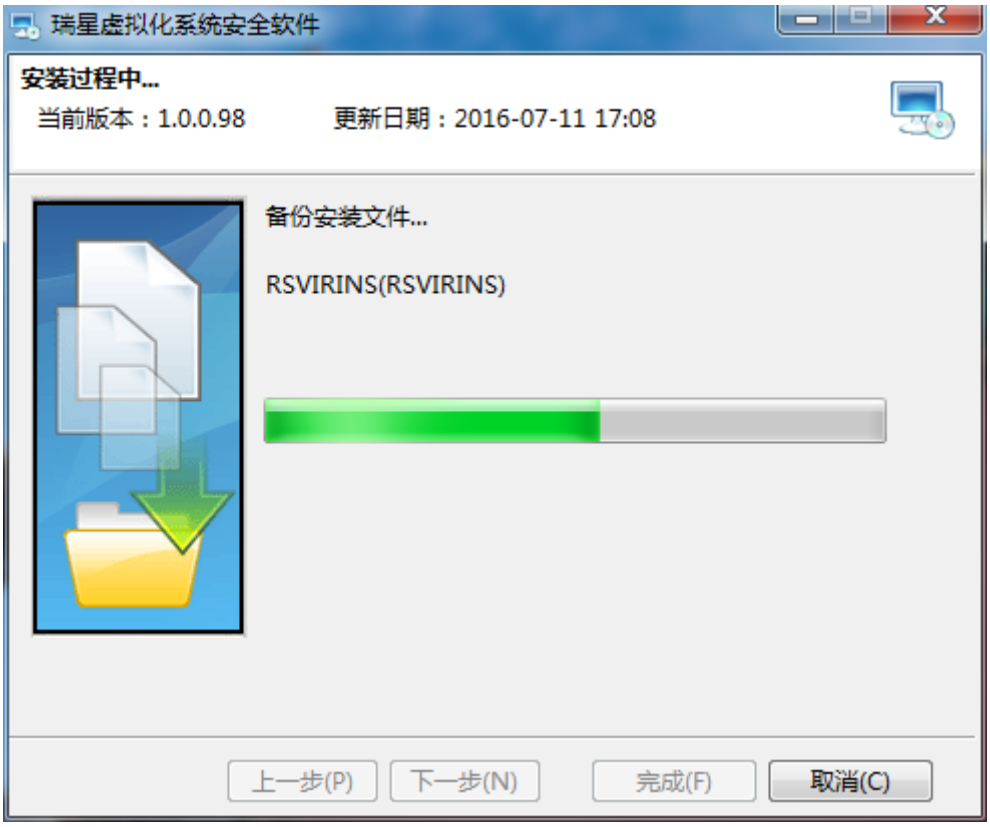
图表 3-84

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



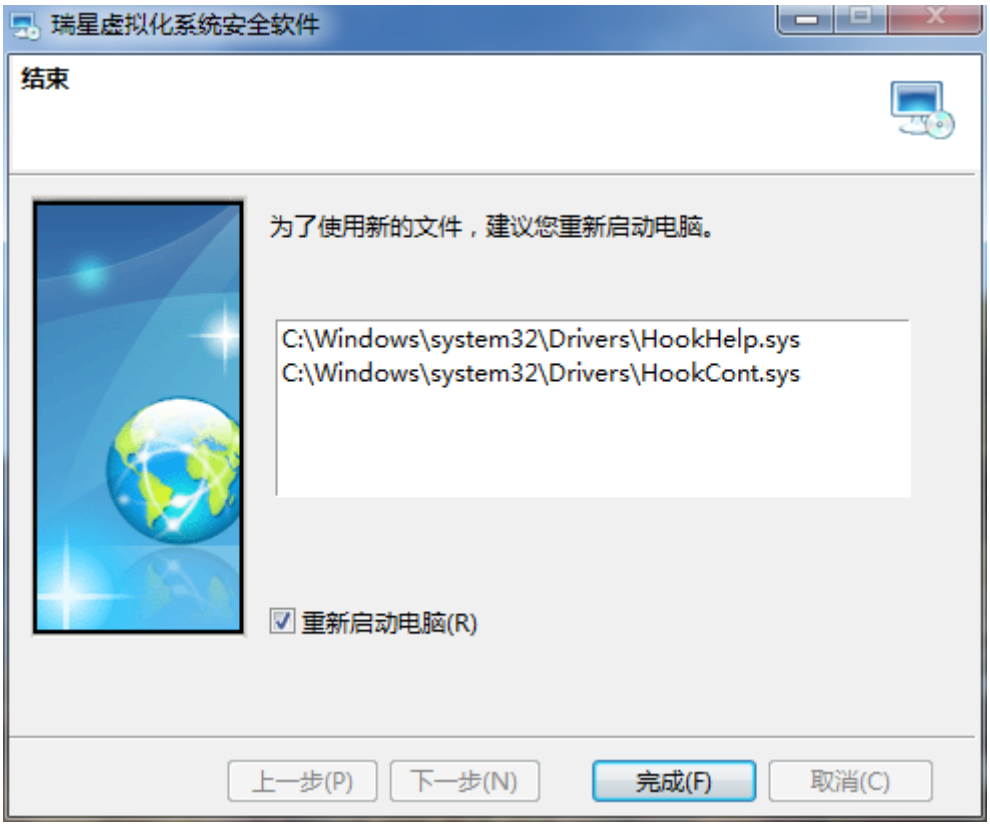
图表 3-85

第八步：安装程序将开始复制文件，完成后单击【下一步】继续。



图表 3-86

第九步：程序安装完成后，单击【完成】按钮，重新启动电脑。

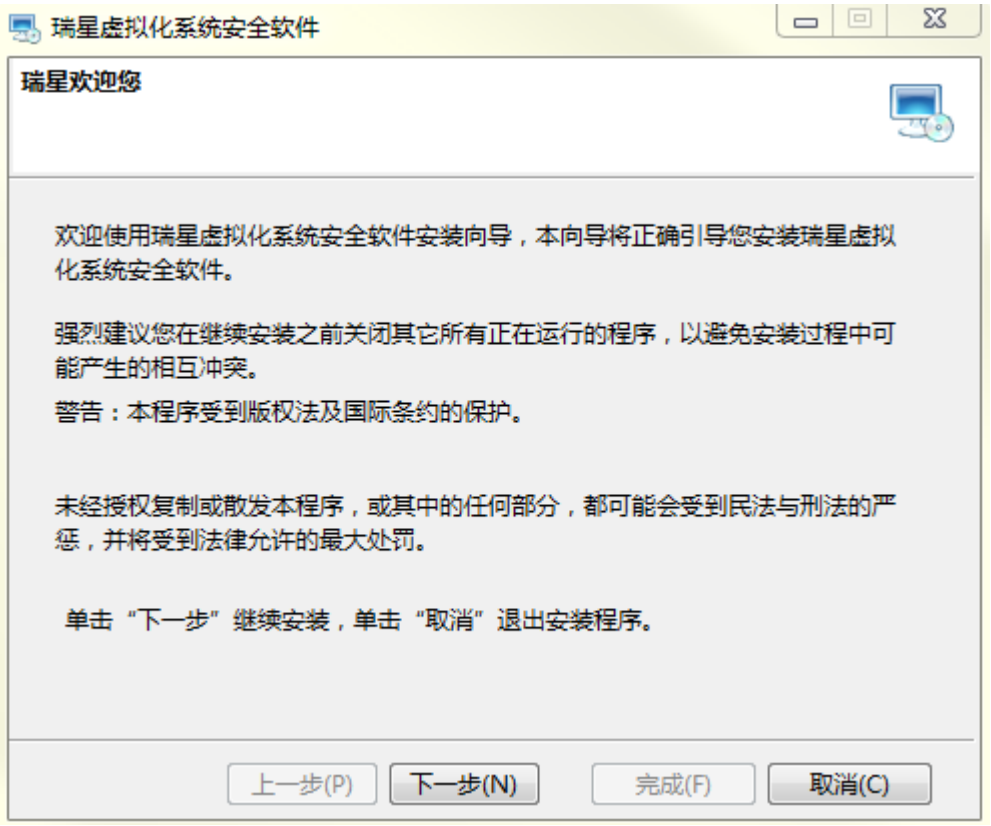


图表 3-87

3.2.8 全功能安全防护客户端

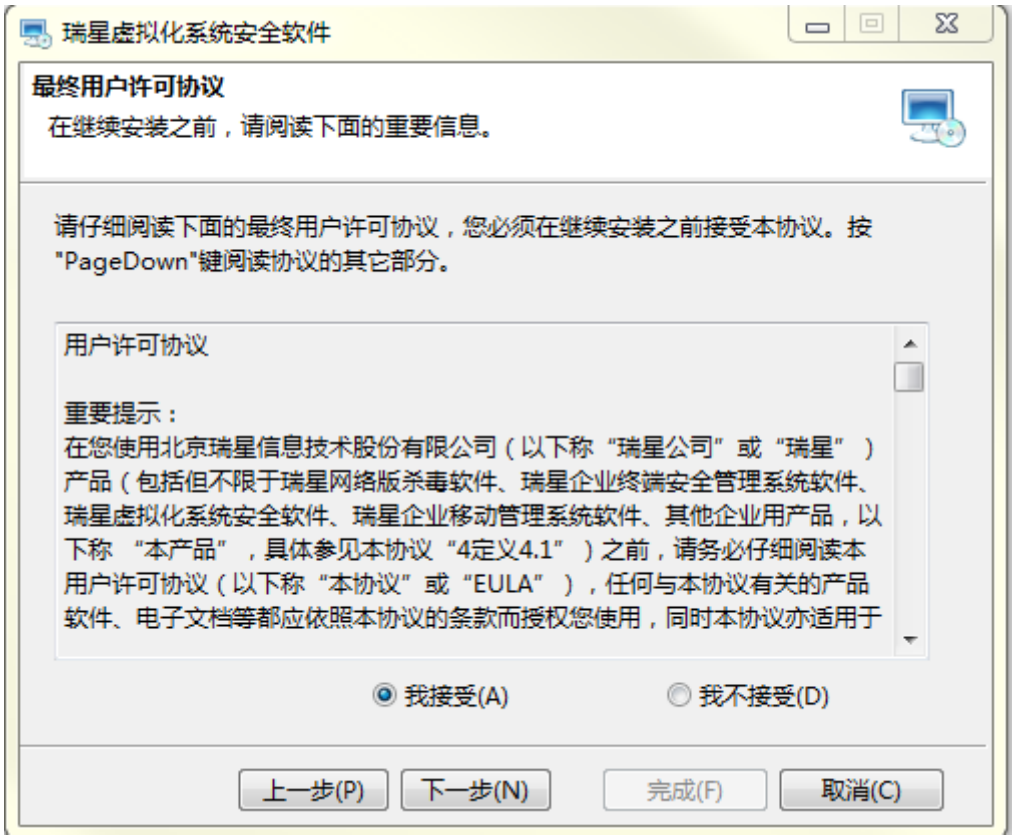
第一步：将瑞星虚拟化系统安全软件光盘放入光驱内进入到全功能安全防护客户端安装包目录下，运行 RVS+VES.exe 安装程序。

第二步：进入安装程序欢迎界面，单击【下一步】继续安装，还可以通过【取消】按钮退出安装过程。



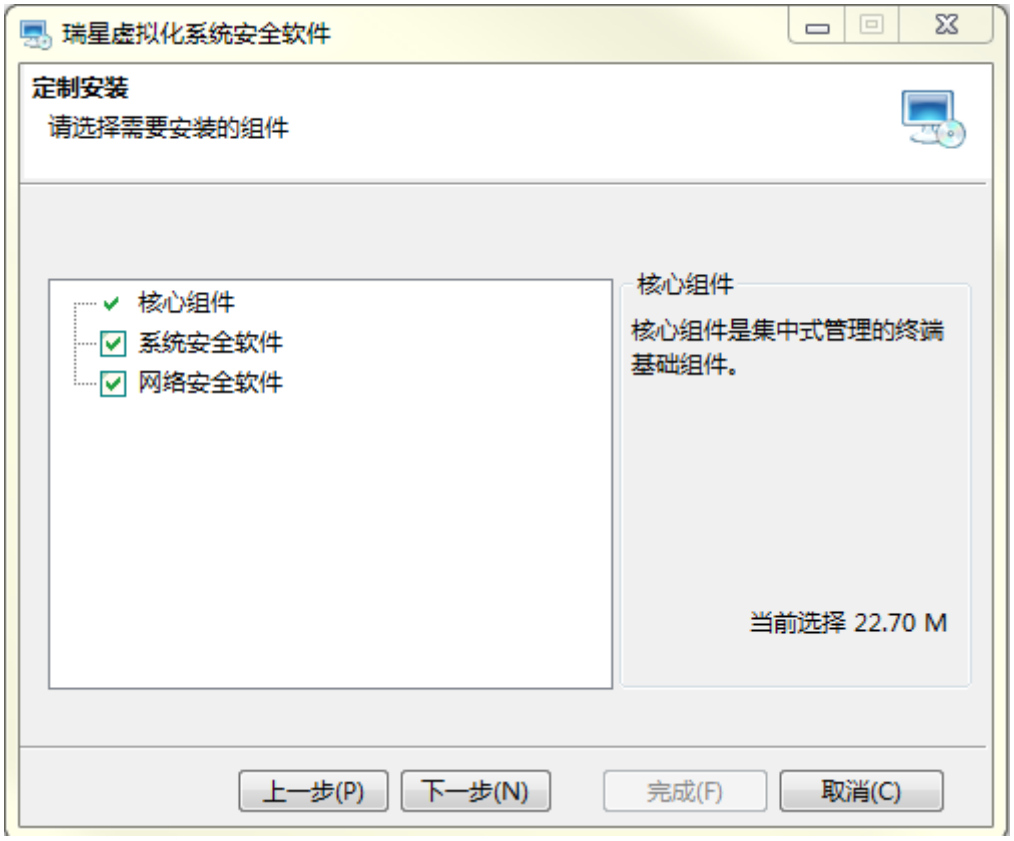
图表 3-88

第三步：弹出【最终用户许可协议】窗口，请仔细阅读软件许可协议。如果接受，请选择【我接受】，单击【下一步】继续安装；如不接受该协议，选择【我不接受】退出安装程序。



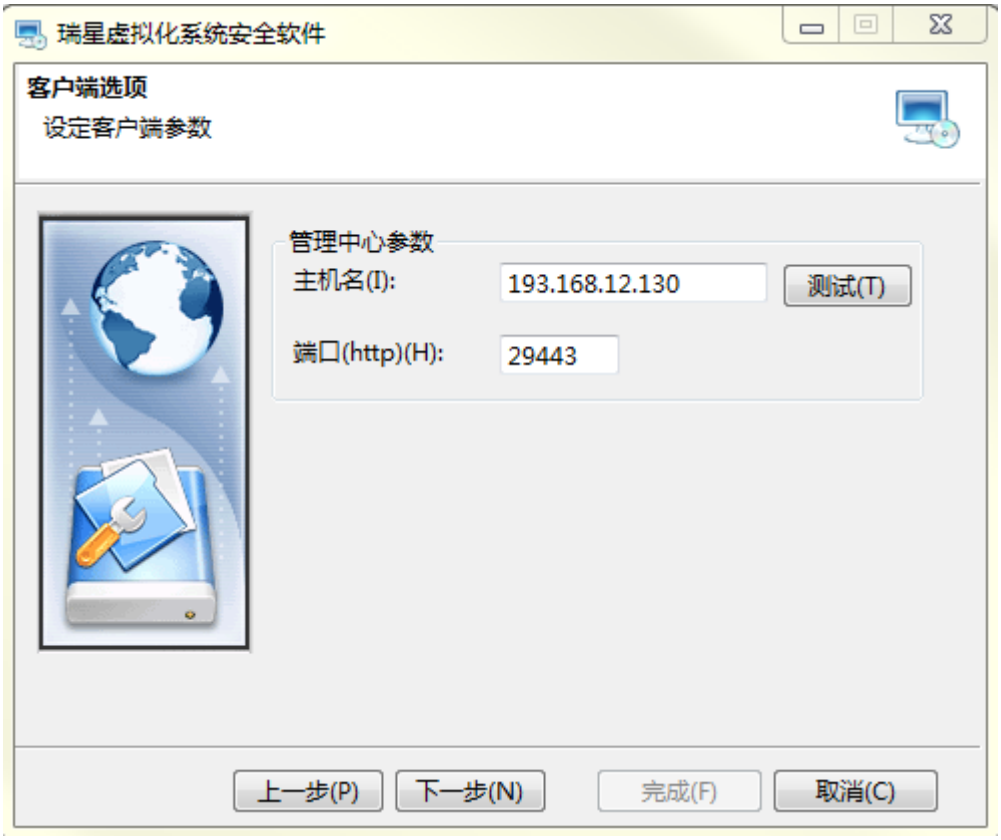
图表 3-89

第四步：进入【定制安装】界面，选择需要安装的【系统安全软件】组件和【网络安全软件】组件，单击【下一步】继续安装。



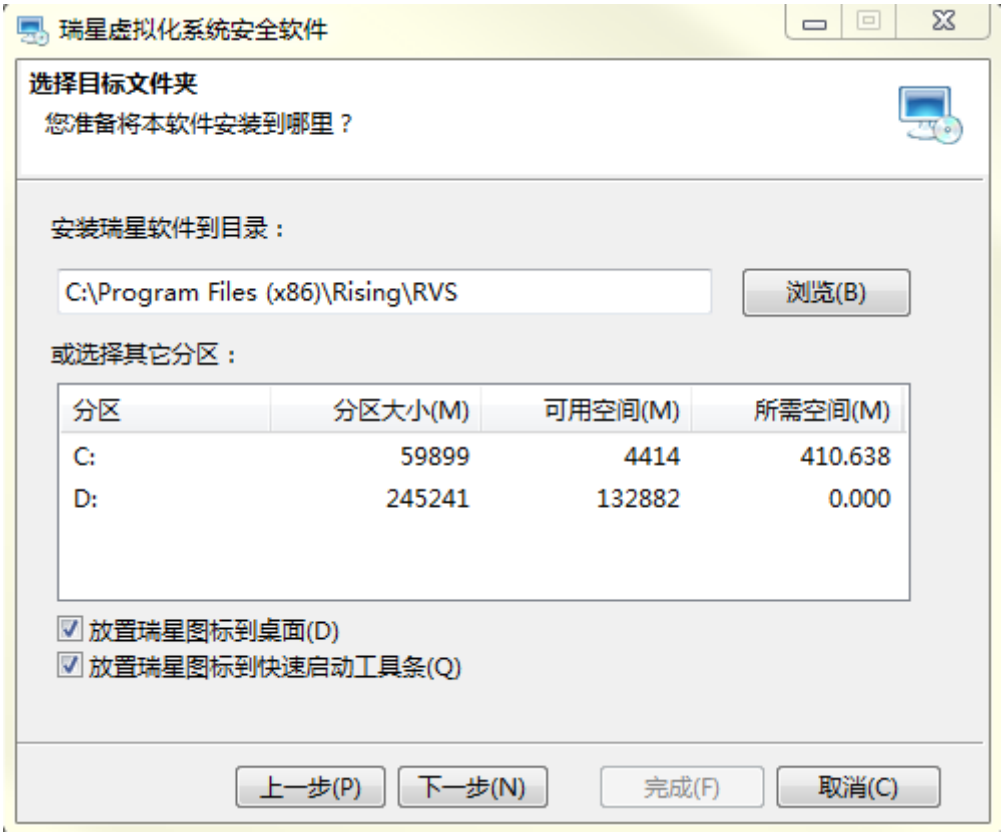
图表 3-90

第五步：进入【客户端选项】界面，指定管理中心 IP 地址，单击【测试】按钮可以测试客户端与管理之间的连通性，单击【下一步】继续安装。



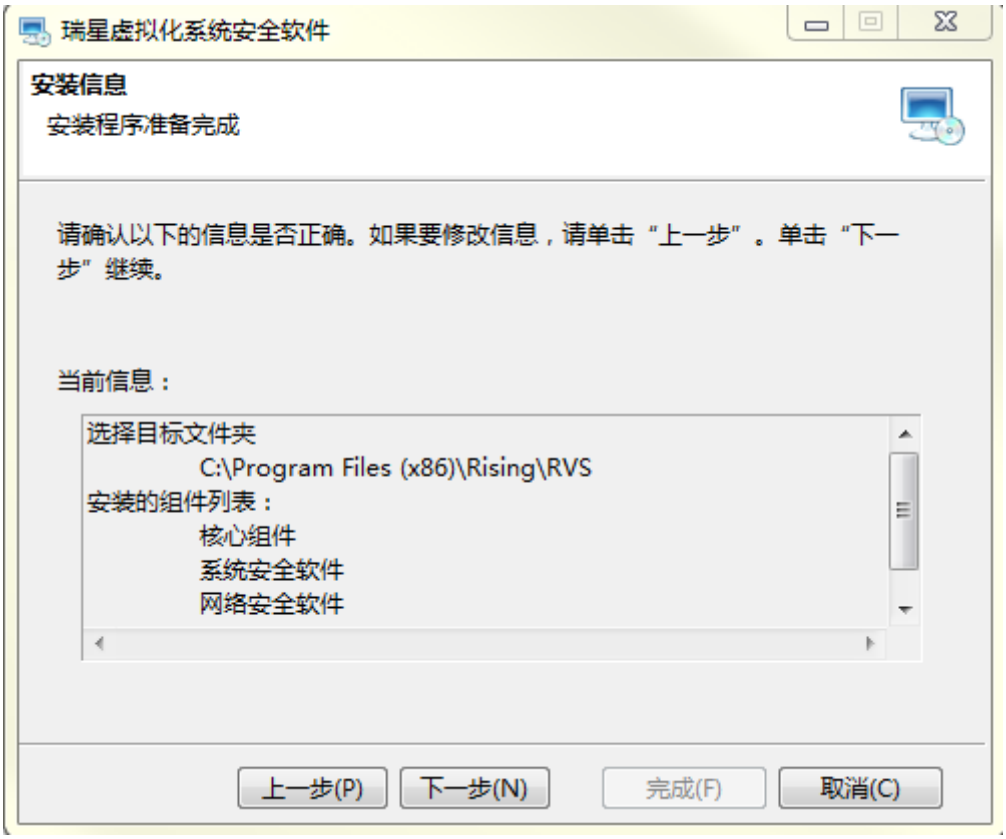
图表 3-91

第六步：在【选择目标文件夹】界面中，选择安装瑞星虚拟化系统安全软件的目标文件夹，勾选【放置瑞星图标到桌面】和【放置瑞星图标到快速启动工具栏】，单击【下一步】继续安装。



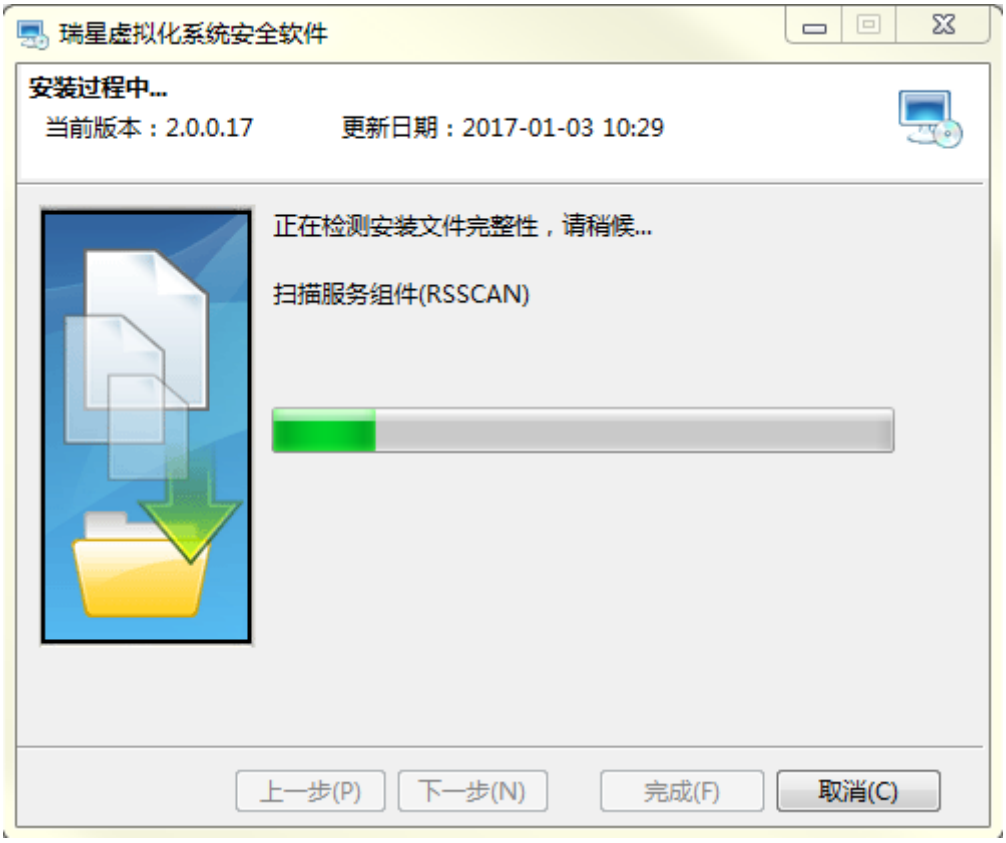
图表 3-92

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



图表 3-93

第八步：安装程序将开始复制文件，完成后单击【下一步】继续。



图表 3-94

第九步：程序安装完成后，单击【完成】按钮，重新启动电脑。

图表 3-95

3.2.9 安全终端 Linux 杀毒

3.2.9.1 字符界面安装

字符界面安装过程中，需要填写瑞星虚拟化系统安全软件管理中心的地址和端口号。

第一步：以 Linux 超级用户身份登录系统。

第二步：将光盘放入光驱中，将瑞星软件光盘正确加载到文件系统中。

第三步：在光盘下，进入到安全终端 Linux 杀毒安装包的目录下，执行光盘下的安装程序./ravsetup text（参数 text），安装程序启动。

```
[root@Red6 CDROM]# ./ravsetup text
Platform is 64-bit OS
Begin to install Rising Rvs2016...
********************************************************************************
*                                                                              *
*                                                                              *
*                  RISING ANTIVIRUS SETUP SOFTWARE                             *
*       COPYRIGHT FOR BEIJING RISING TECHNOLOGY CO.,LTD. 2015-2016             *
*                                                                              *
********************************************************************************
Please input the installing path(must be absolute path),You can install RISING A
NTIVIRUS SOFTEARE in
["/usr/rav" by Typing Enter]>
```

图表 3-96

第四步：根据提示输入安装目录的绝对路径（也可以使用默认目录/usr/rav/），回车。确认创建目录程序开始复制文件，输入“y”，回车。

```
["/usr/rav" by Typing Enter]>
Directory "/usr/rav" does not exist!
Do you want create it ?
[ y ]  : Create directory "/usr/rav"
[ n ]  : Exit the setup
y
Setup file bin/pmcupdate
Setup file bin/ravcmdupdate.bin
Setup file bin/pmcagent
```

图表 3-97

第五步：文件复制完成后，根据程序提示输入瑞星虚拟化系统安全软件管理中心管理中心地址信息。这里以 https://193.168.12.130:29443 为例。输入完成，回车。

```
************************************************************
*                                                          *
*                Please input Center URL                   *
*        For Example:  https://193.168.12.130:29443        *
*                                                          *
************************************************************
Center URL>https://193.168.12.130:29443
Add self-loading information of program ..............ok !
Add service.............ok!
Add pmcagent.............ok!
Add esmagent.............ok!
```

图表 3-98

第六步：安装程序进行网络初始化，提示杀安全终端 Linux 杀毒启动成功。

```
Start ravservice Ok
```

图表 3-99

产品安装结束后安装路径中主要目录及文件清单。

目录名称	文件名称	说明	注意事项
bin		瑞星虚拟化系统安全软件 For UNIX 所有执行程序所在目录	
	rav	本地用户字符界面程序	
	chinrav	中文语言包程序	
	englrav	英文语言包程序	
	ravUNIX	本地用户图形版杀毒主界面程序	
	ravlog	本地用户图形版日志界面程序	
	ravqua	本地用户图形版隔离系统界面程序	
	ravservice	网络版客户端常驻服务程序	
	ravupdate	本地用户图形版升级界面程序	
	ravcmdupdate	本地用户字符升级程序	
	upcenter	用于从管理中心以智能包方式升级	
	setupini	用于注册或修改所连接的管理中心和设置升级方式的程序	
	risingscan	本地扫描查杀程序	
	ravcmdscan	定时扫描查杀程序	
	ravscan	网络版客户端查杀程序	
	rscfg	修复网络客户端 RsConfig.cfg 配置文件	
	start.sh	随机启动服务的脚本	
	ravunsetup	本地用户卸载程序	请在根目录执行此程序
	ravcmdunsetup	本地用户字符版卸载程序包	
	ravguiunsetup	本地用户图形版卸载程序包	
etc	ravqua.ini	隔离系统的配置文件	
Ravnet		网络版客户端配置信息所在父目录	
Ravnet/sys		网络版客户端配置文件所在目录	
	ravservice.log	Ravservice 日志	
	ravservice.sys	Ravservice 配置文件	
	RsConfig.cfg	网络版客户端查杀配置文件	
	ravservice.ini2	客户端配置文件	在此文件中修改查杀目录
Ravnet/version		网络版客户端版本信息目录	
	version.ini	网络版客户端版本信息文件	
ravsingle		本地操作目录	
ravsingle/conf		本地配置文件目录	
	rav.ini	字符主程序 rav 的配置文件	
	Risingparam	查杀程序的配置文件（在客户端设置后生成）	
ravsingle/rhelp		帮助文件所在目录	

目录名称	文件名称	说明	注意事项
ravsingle/version		本地版本信息目录	
	version.ini	本地版本信息文件	
ravgui		本地图形版配置文件所在目录	
ravgui/etc		本地图形版设置文件所在目录	
	ravUNIX.ini	图形版配置文件	
ravgui/resource		图形版资源所在目录	
ravgui/resource/help		图形版帮助资源所在目录	
ravgui/resource/image		图形版图片资源所在目录	
ravgui/resource/lang		图形版语言资源所在目录	
version		图形版主界面上显示版本目录	
	version.ini	图形版主界面上显示版本文件	
log		升级日志，查杀日志	
virusdb		病毒库文件所在目录	
	*.def	病毒库文件	
	virusdu.cfg	病毒库配置文件	
virbak		默认的病毒隔离区目录	

图表 3-100

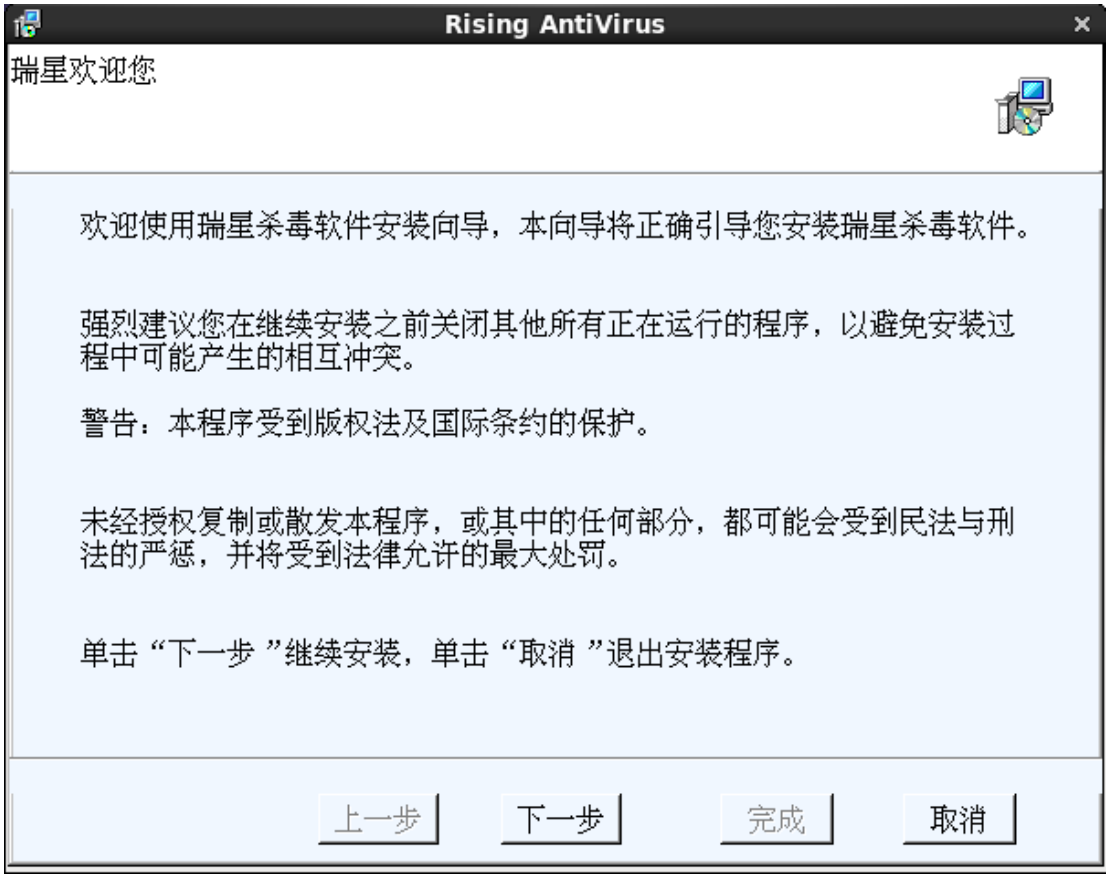
3.2.9.2 图形界面安装

第一步：在 UNIX/Linux 的图形界面下，进入到光盘中安全终端 Linux 杀毒的安装包路径下，运行：./ravsetup，进入图形版的安装，依照界面的提示进行下一步安装；

```
[root@Red6 CDROM]# ./ravsetup
Platform is 64-bit OS
Begin to install Rising Rvs2016...
```

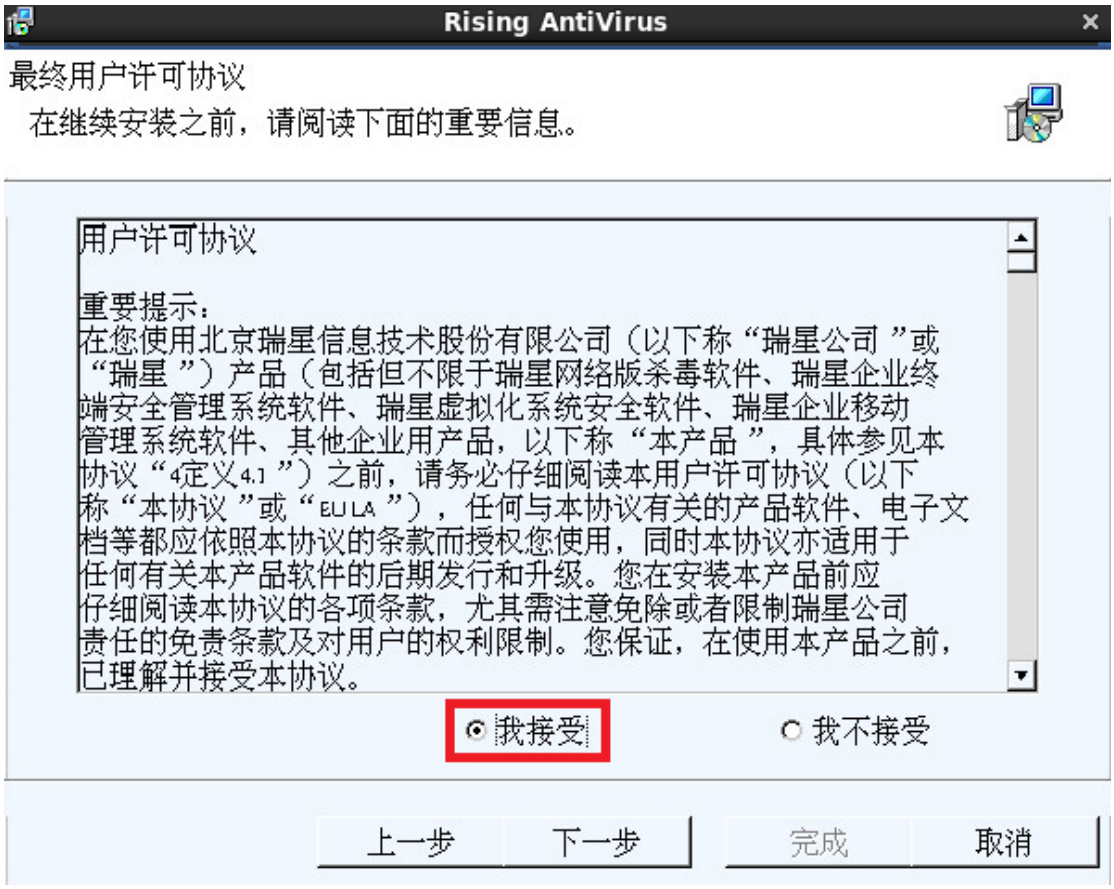
图表 3-101

第二步：进入安装欢迎界面；



图表 3-102

第三步：阅读【最终用户许可协议】，选择【我接受】；

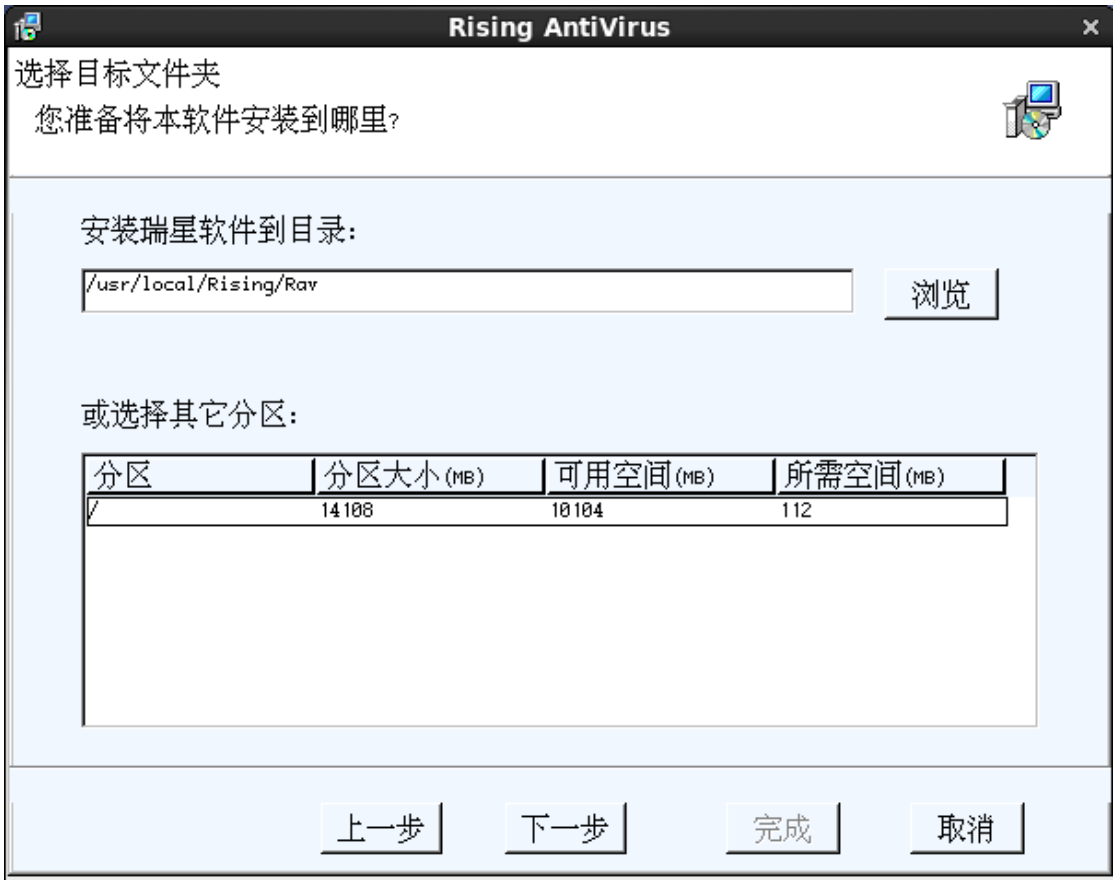


图表 3-103

第四步：在管理中心设置输入管理中心 URL 和端口号，点击下一步；

图表 3-104

第五步：自定义产品安装路径，点击【下一步】。

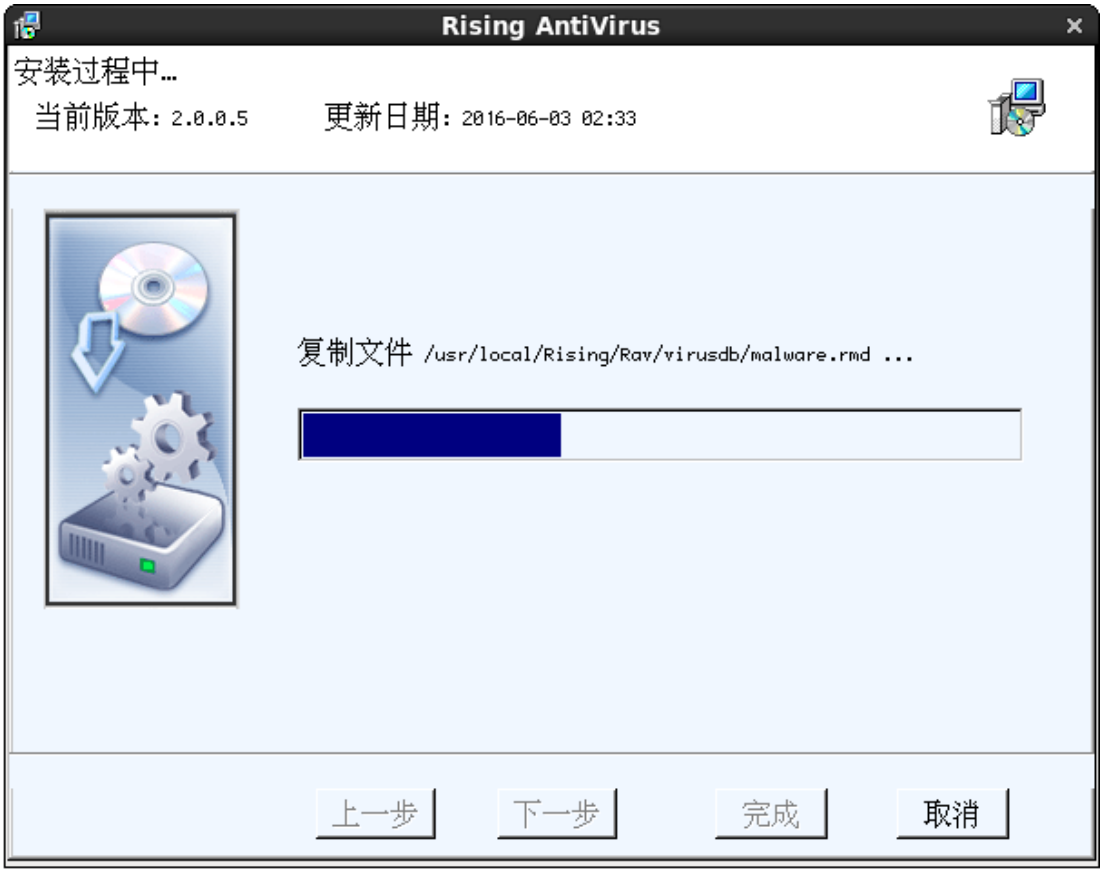


图表 3-105

第六步：确认安装信息，点击【下一步】。

图表 3-106

第七步：安装过程中，复制文件大概需要几分钟到十几分钟，时间长短依赖于设备环境。



图表 3-107

第八步：文件复制完成后，提示产品成功安装到计算机中，在桌面将出现产品图标 

。

提示：只有在root账户登录的情况下，才能在桌面看到软件图标，普通账户请到对应账户目录/home/username下查看图标。

3.2.10 Linux 全功能防护客户端

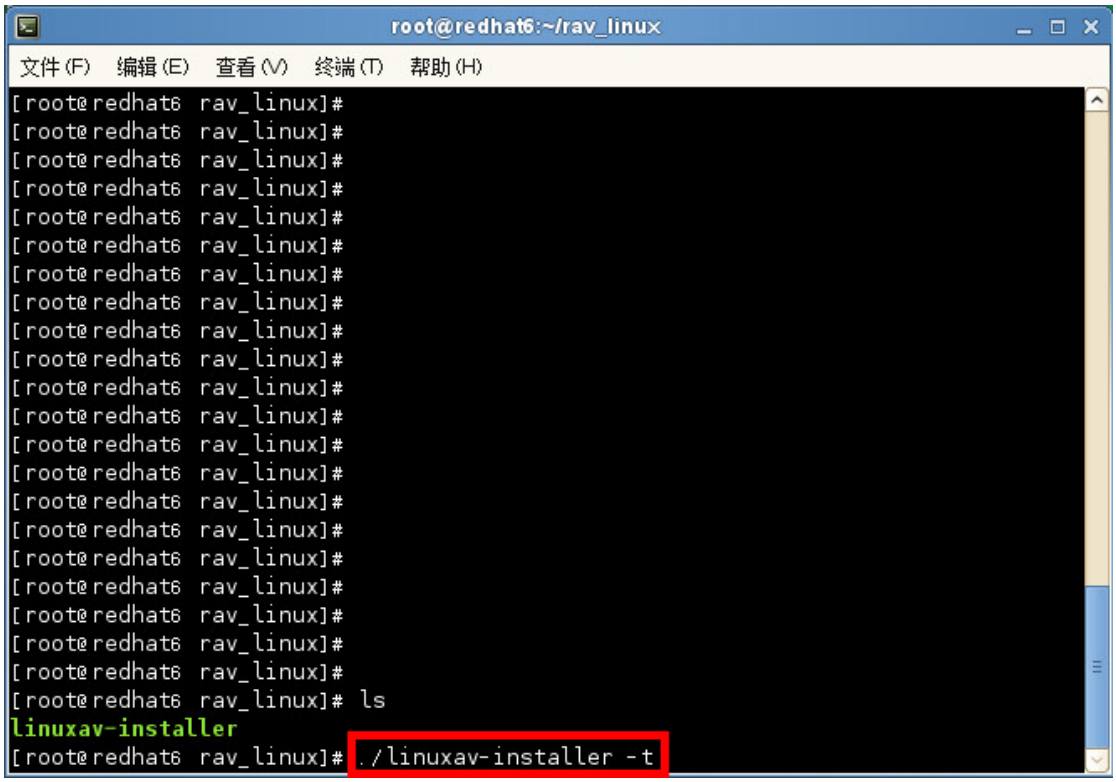
3.2.10.1 字符界面安装

对于绝大多数 Linux 系统而言，都可以在桌面环境上安装 Linux 全功能防护客户端，但对于一些少数的系统，可能不能够在桌面环境下进行安装，这些系统或者没有安装桌面环境，或者缺少软件在桌面环境下运行所依赖的必要库文件等（如 libqt4），这些系统可以尝试在字符界面下进行安装，下面说明字符界面安装步骤。

1、 将 Linux 杀软的安装光盘挂载后，打开一个终端窗口，到光盘目录运行安装程

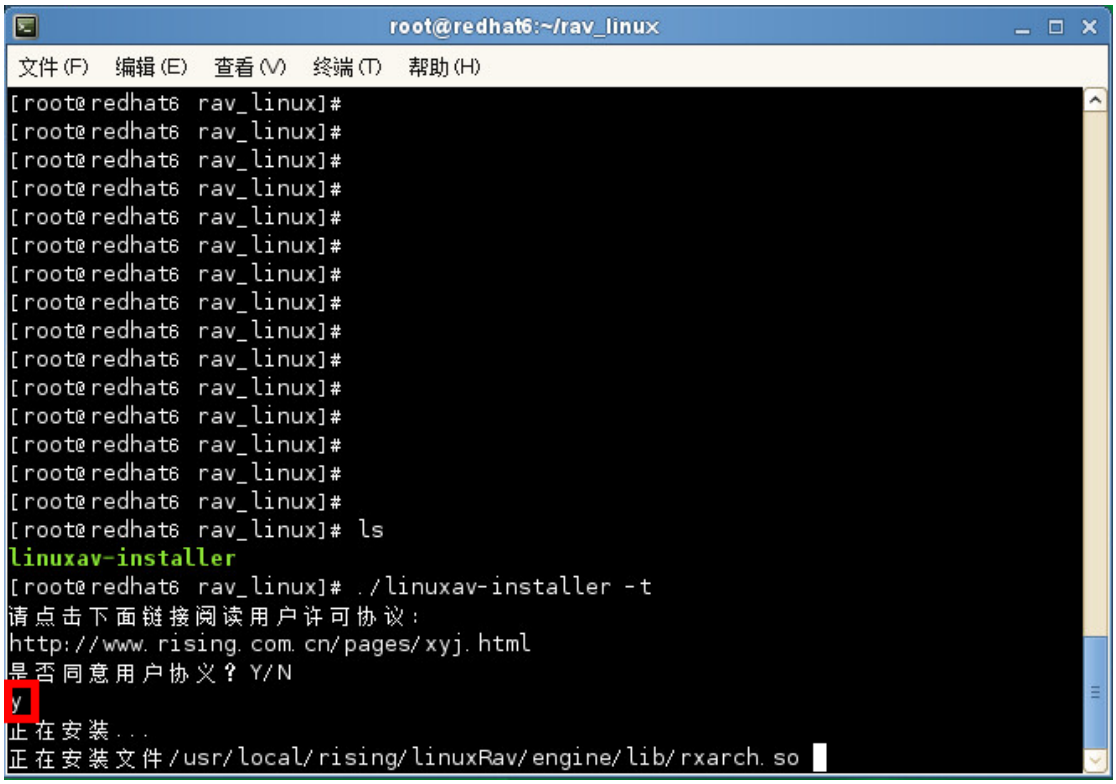
序./Linuxav-installer -t 进行安装。

注意：运行安装程序需要root权限。



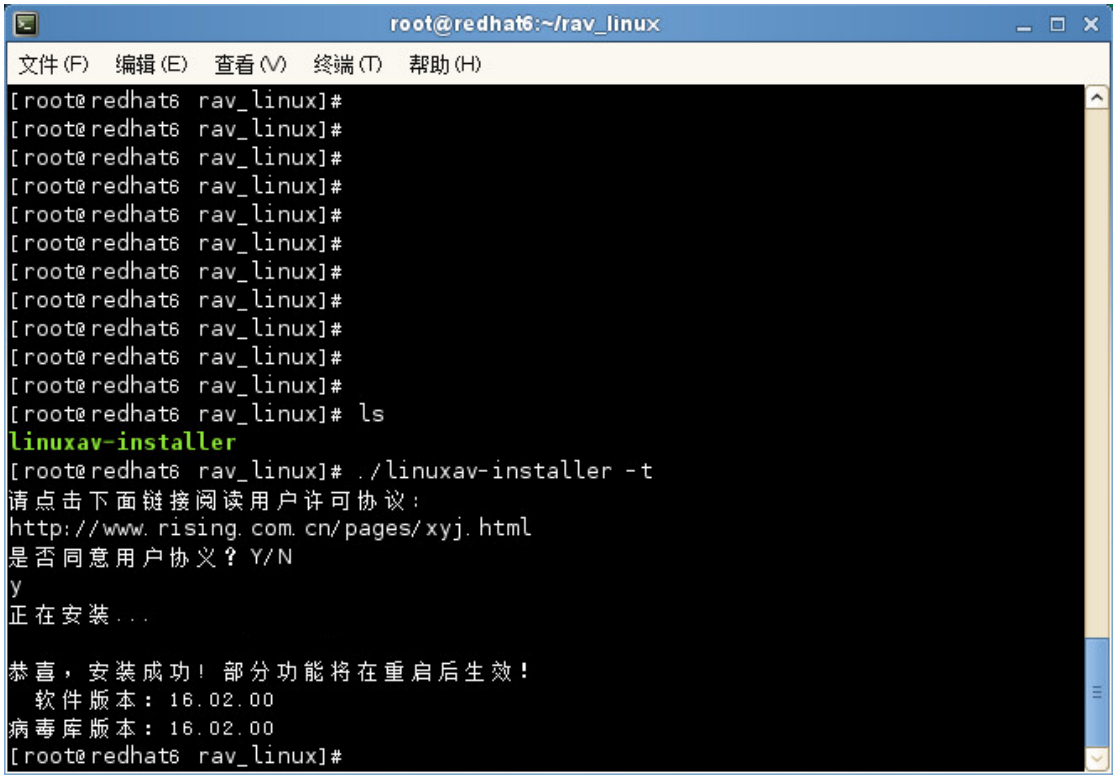
图表 3-108

2、 在终端中将显示出写有瑞星杀毒软件版权信息的 web 页面，用户可通过此页面浏览版权信息。在此处输入“y”并按回车，开始安装。

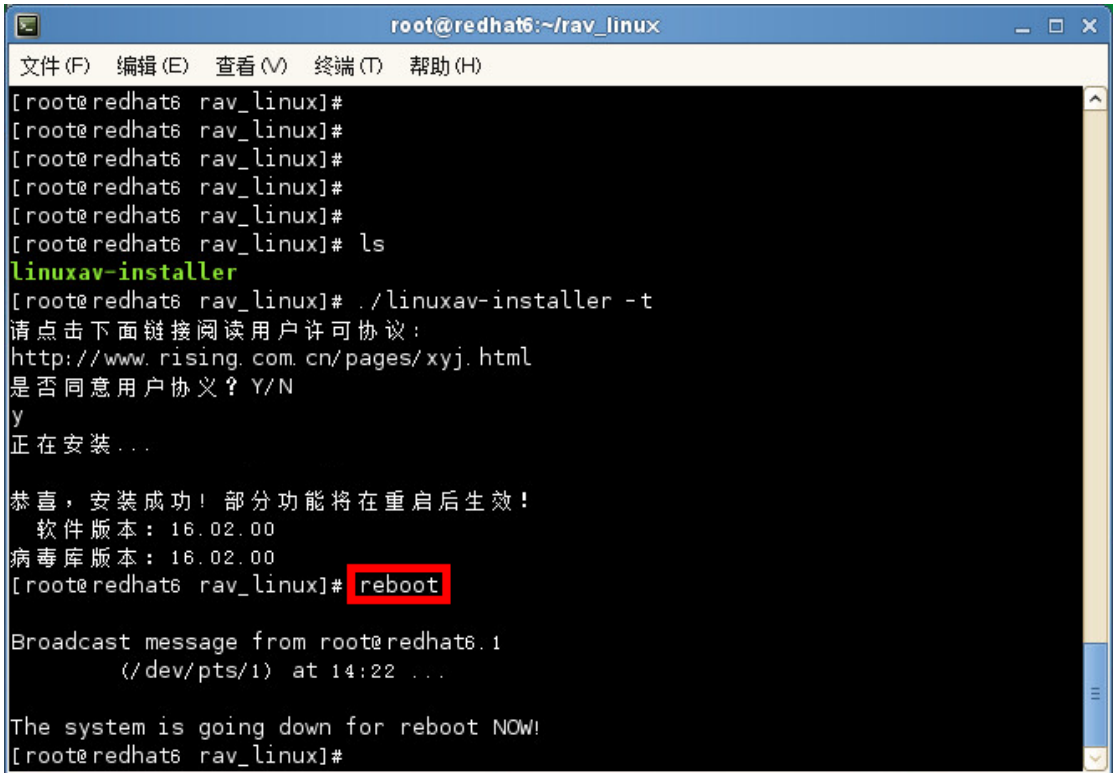


图表 3-109

3、 安装结束后，会出现“恭喜，安装成功！部分功能将在重启后生效！”，这时用户可重启系统来完成安装。



图表 3-110



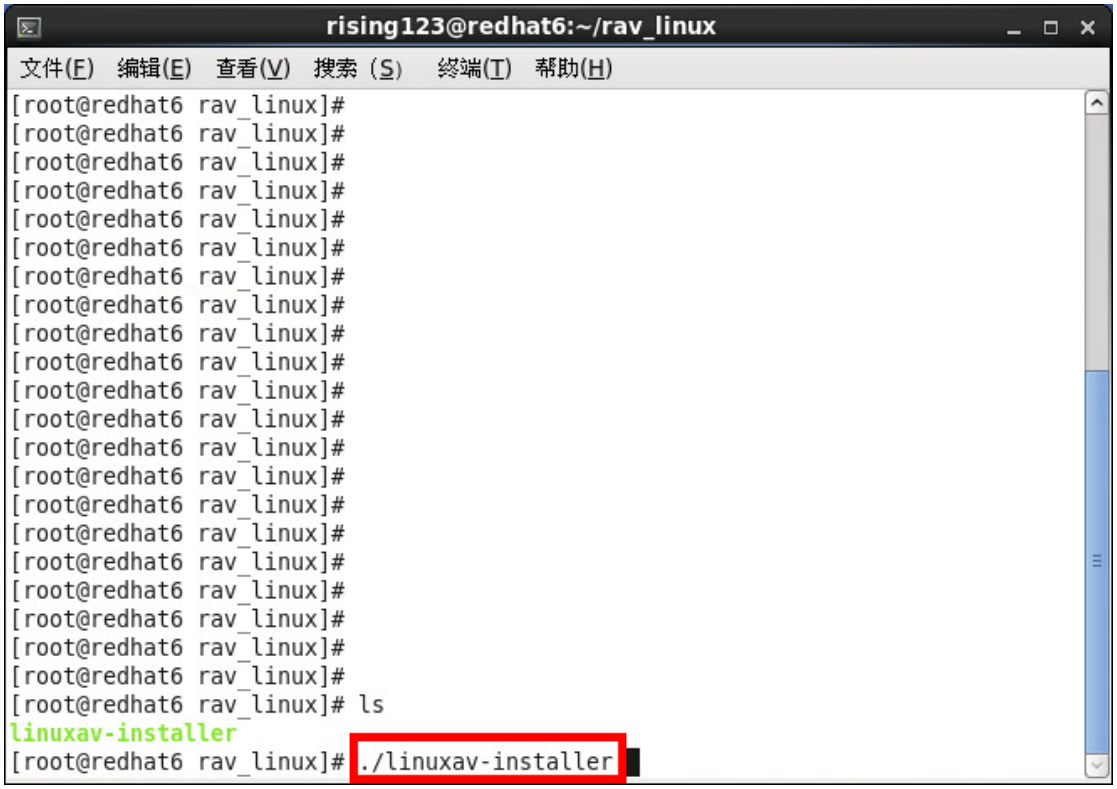
图表 3-111

至此，字符界面下安装过程结束。

3.2.10.2 图形界面安装

1、 将瑞星杀毒软件 for Linux 的安装光盘挂载后，打开一个终端窗口，到挂载光盘目录运行安装程序**./Linuxav-installer** 进行安装。

注意：运行安装程序需要root权限。



图表 3-112

2、 在打开的安装窗口中，勾选“我已经阅读并同意瑞星许可协议”的版权信息，点击“开始安装”进行安装。安装页面显示的产品名称是随用户系统而变化的，对于能识别系统，则显示系统名称，对于无法识别的系统，则统一显示为 For Linux。本文档以红帽 6 及以上或相类似的系统为例进行说明。

注意，程序默认安装路径为/usr/local/rising/LinuxRav。

图表 3-113

注意，如果界面出现信息“安装失败！请使用root权限安装”说明运行安装程序的用户没有root权限，请获得权限后再次运行安装程序。

图表 3-114

3、 如果权限正常，软件将开始安装，并且在界面提示正在安装的文件信息。

图表 3-115

4、 待软件安装完成后，会提示用户重启系统，用户可选择“立即重启”或“稍后重启”，这里我们点击“立即重启”。

图表 3-116

5、 重启系统后，安装过程结束。如果用户以 root 账号登录系统，可在桌面找到“瑞星

杀毒图标”“ 

”；如果用户以普通账号登陆系统，用户可通过文件浏览器在/home 下找到“瑞星杀毒图标”。

6、 至此安装结束。

3.3 组件授权

瑞星虚拟化系统安全软件组件包括管理控制中心、VMware 无代理杀毒、HUAWEI 无代理杀毒、安全防护终端、全功能安全防护客户端、安全终端 Linux 杀毒和 Linux 全功能防护客户端，各组件采用统一的授权方式。

提示：VMware的SVM，授权导入后需要手动激活。华为的SVM，授权导入后不需要手动激活。

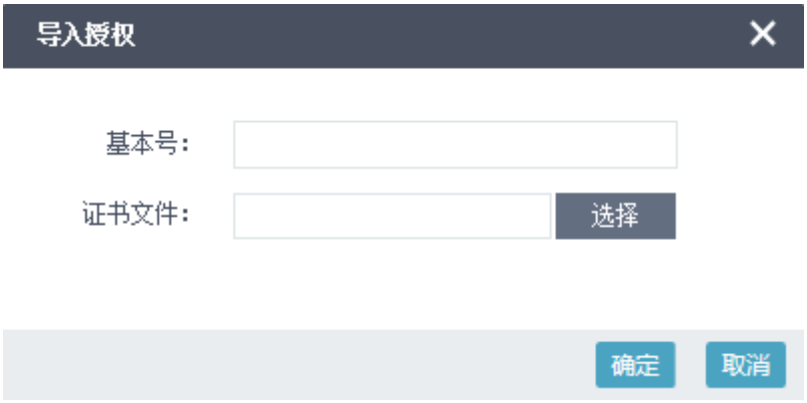
3.3.1 导入授权证书

第一步：点击管理中心的【系统管理】/【授权证书】，显示授权证书页面。

提示：授权证书的获取方式，请参考本文档章节3.1.2 产品序列号。

图表 3-117

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 3-118

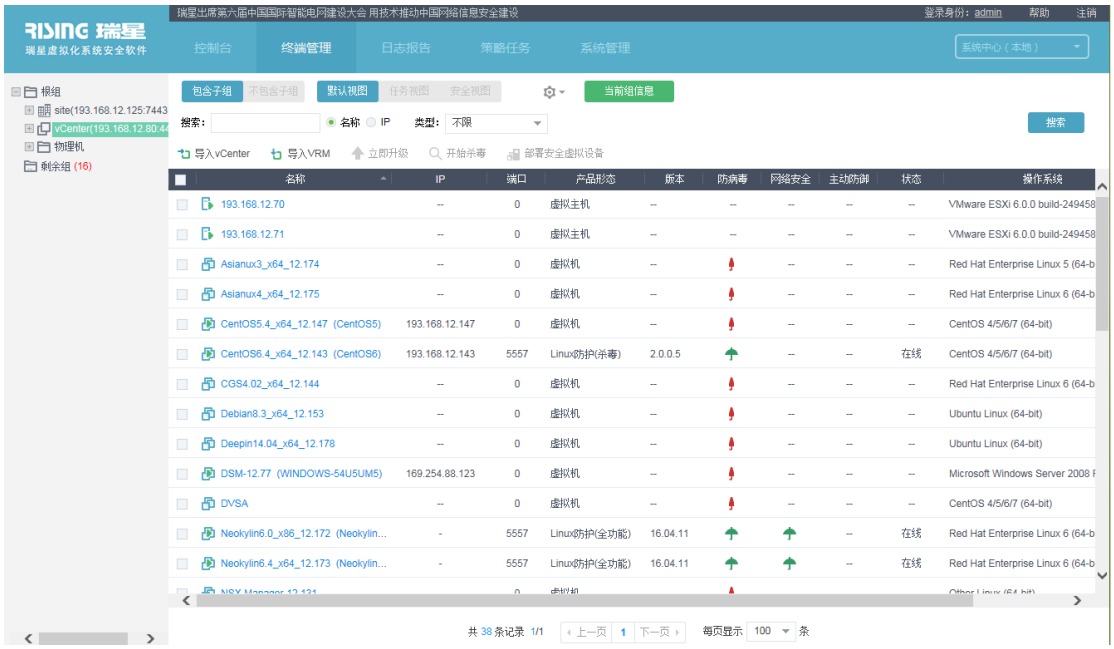
第三步：确定导入授权后，在【授权证书】页面显示授权许可的详细信息，导入后，该产品授权为“有效”状态。

管理控制中心	2016/05/19 至 2019/05/20	1	1	有效	详情
VMware无代理杀毒	2016/05/19 至 2019/05/20	10	2	有效	详情
Huawei无代理杀毒	2016/05/19 至 2019/05/20	10	2	有效	详情
Linux防护(杀毒)	2016/05/19 至 2019/05/20	20	3	有效	详情
Linux防护(全功能)	2016/05/19 至 2019/05/20	20	2	有效	详情
终端防护(虚拟桌面)	2016/05/19 至 2019/05/20	100	0	有效	详情
终端防护(客户端)	2016/05/19 至 2019/05/20	50	2	有效	详情
终端防护(服务器)	2016/05/19 至 2019/05/20	50	1	有效	详情

图表 3-119

3.3.2 激活 VMware 安全虚拟设备（vShield）

第一步：点击【终端管理】标签页/【vCenter】组，显示终端设备。

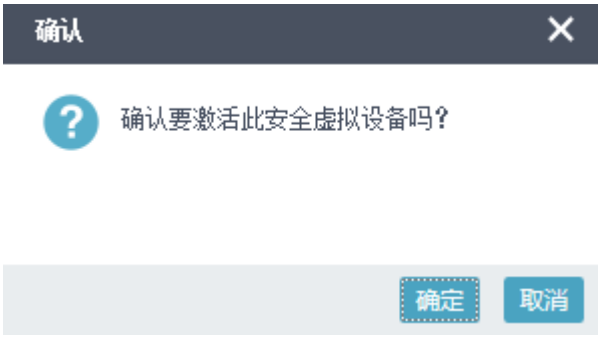


图表 3-120

第二步：点击安全虚拟设备，显示其激活状态。

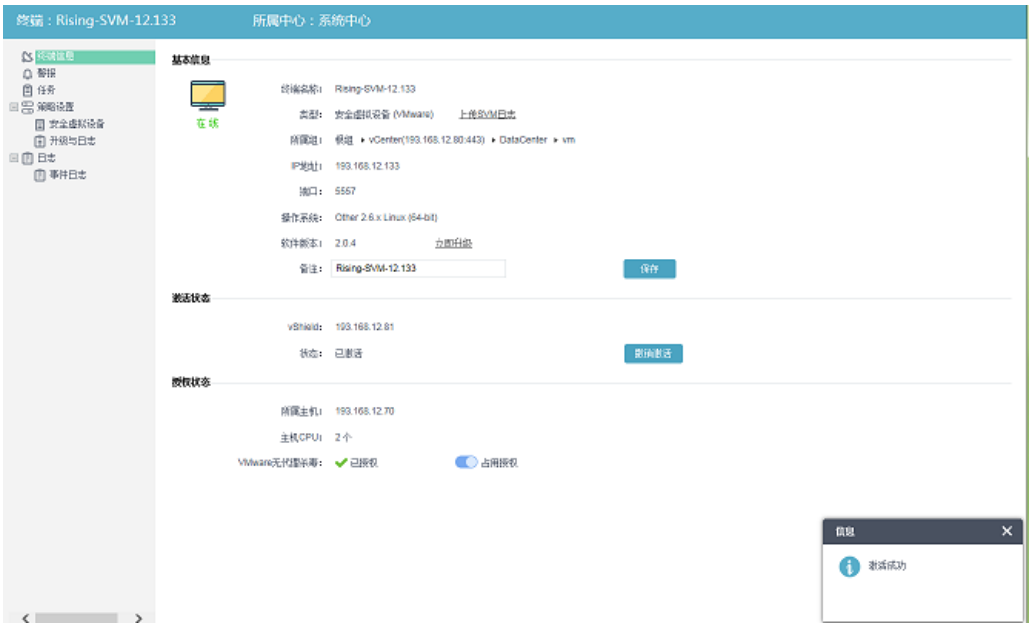
图表 3-121

第三步：点击【激活】按钮，确定激活安全虚拟设备。



图表 3-122

第四步：激活完成后，右下角弹出窗口提示：“激活成功”。

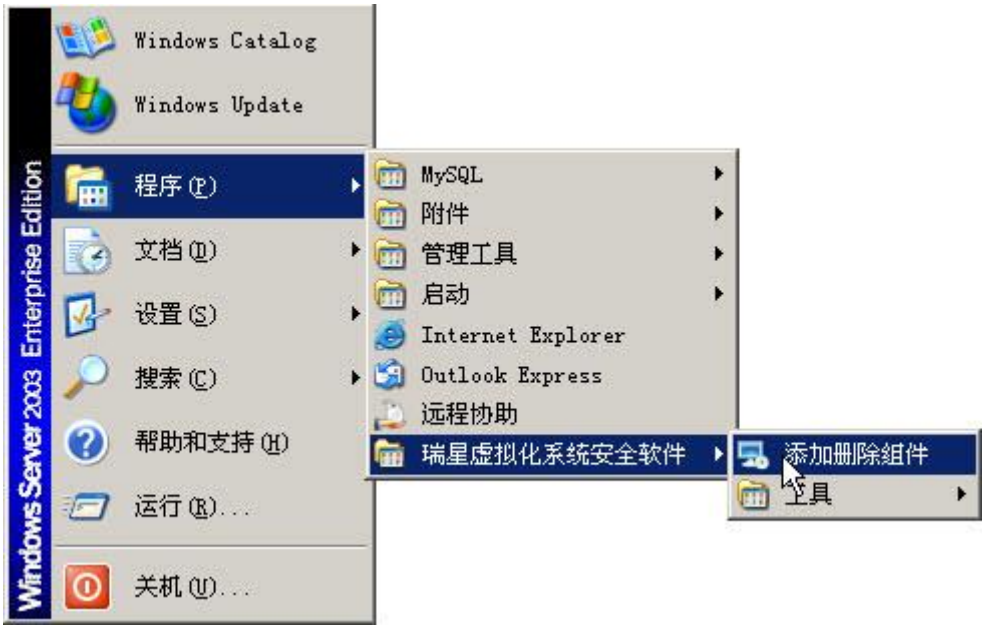


图表 3-123

3.4 组件卸载

3.4.1 中心与 RSTools

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】。

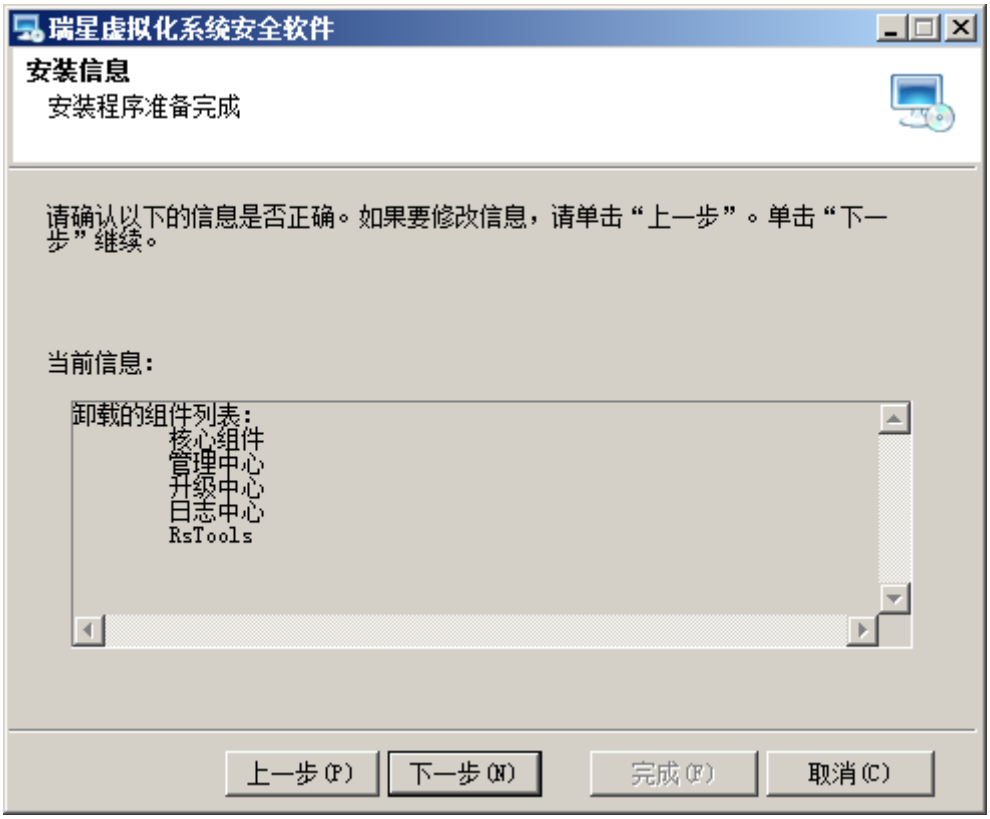


图表 3-124

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 3-125

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 3-126

第四步：显示卸载进度信息。

图表 3-127

第五步：点击【完成】，卸载结束。

图表 3-128

3.4.2 VMware 安全虚拟设备

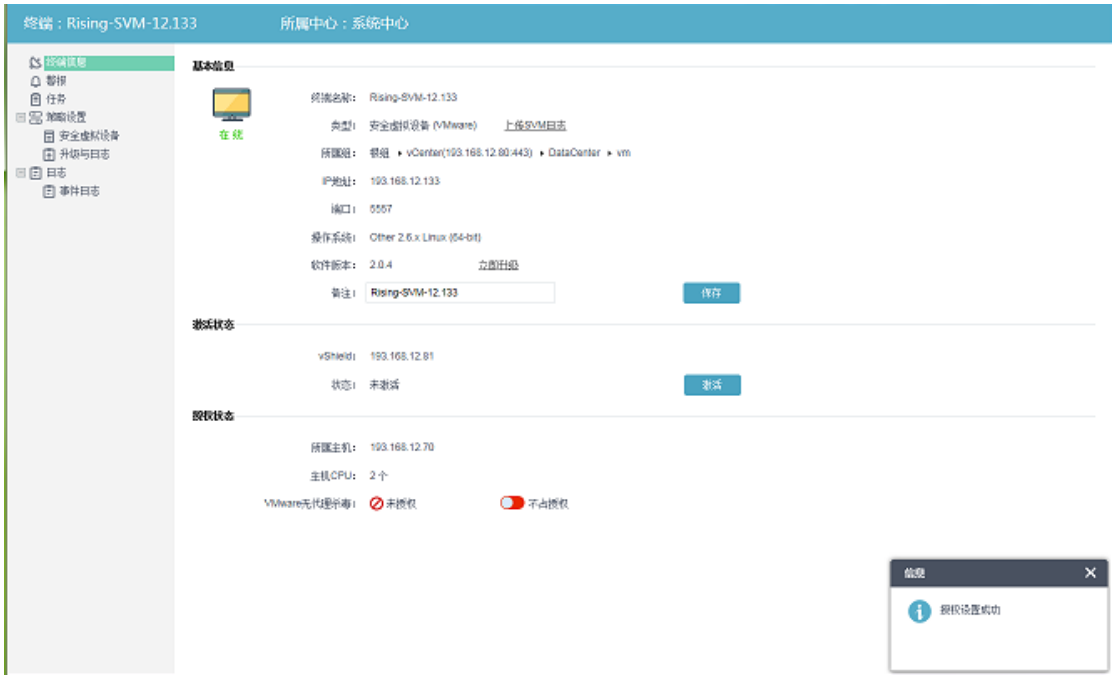
第一步：点击控制台导航窗口的【终端管理】/【vCenter 终端】，在终端窗口中点击安全虚拟设备，显示其激活状态和授权状态。

图表 3-129

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 3-130

第三步：选择 VMware 无代理杀毒【占用授权】，点击【确定】按钮，右下角弹出窗口提示："授权设置成功"。

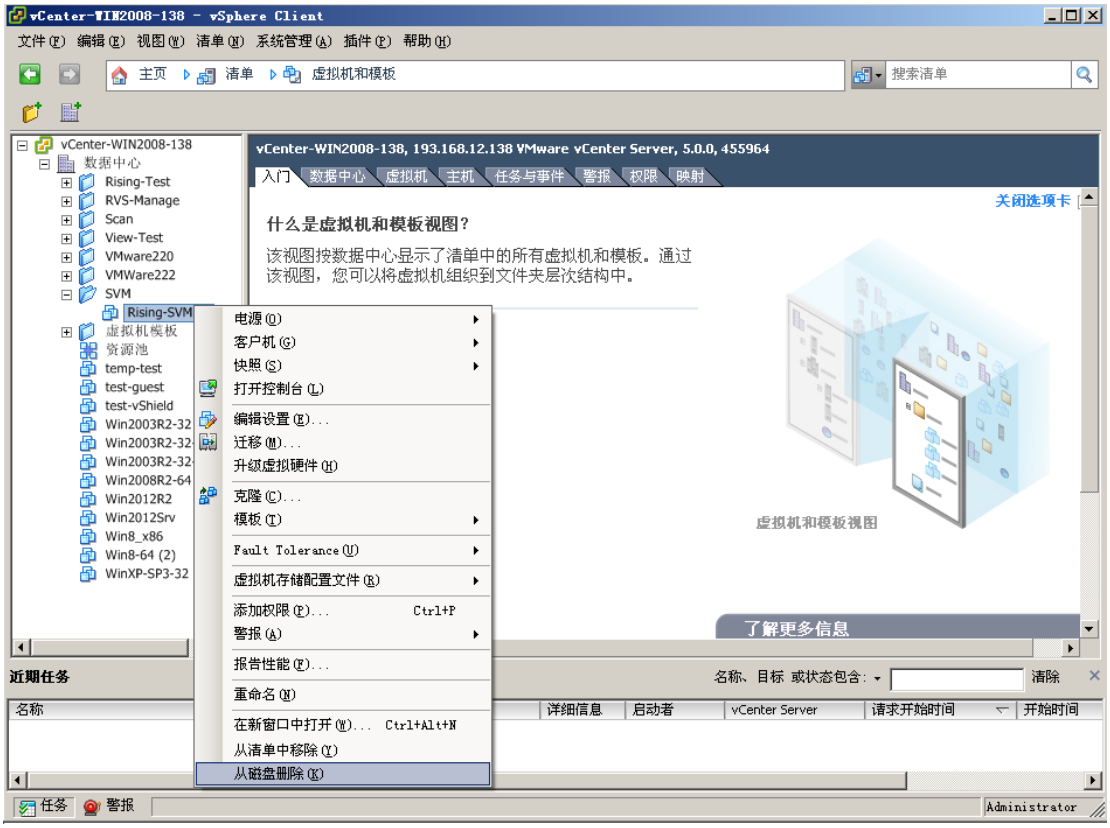


图表 3-131

提示：只能为开启授权状态的安全虚拟设备撤销授权。

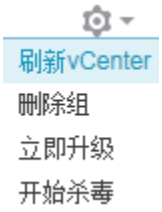
第四步：登录到 vCenter，在 vSphere Client 界面左侧树形结构中，选中待卸载的安全虚拟设备的图标，点击右键，弹出快捷菜单。选择【从磁盘删除】，在弹出的删除确认窗口点

击【是】，完成删除安全虚拟设备的操作。



图表 3-132

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 3-133

3.4.3 HUAWEI 安全虚拟设备

第一步：点击控制台导航窗口的【终端管理】/【VRM 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 3-134

第二步：选择 HUAWEI 无代理杀毒【占用授权】，点击【确定】按钮，右下角弹出窗口提示：“授权设置成功”。

图表 3-135

提示：只能为开启授权状态的安全虚拟设备撤销授权。

第三步：登录华为虚拟化管理平台，切换到“虚拟机和模板”管理界面，选中待卸载的安全虚拟设备虚拟机，点击“更多”，弹出快捷菜单。选择“安全删除”，在弹出的删除确认窗口

点击“立即删除”，完成删除安全虚拟设备。

第四步：点击管理控制台目录下的 VRM，点击右上角【刷新 VRM】，终端列表中不再出现待卸载的安全虚拟设备。

图表 3-136

3.4.4 安全防护终端

3.4.4.1 客户端本地卸载

在 Windows 桌面，选择【开始】/【程序】/【瑞星虚拟化系统安全软件】/【添加删除组件】，在弹出的【瑞星软件维护模式选项】界面中选择【卸载】。

3.4.5 全功能安全防护客户端

在 Windows 桌面，选择【开始】/【所有程序】/【瑞星虚拟化系统安全软件】/【添加删除组件】，在弹出的【瑞星软件维护模式选项】界面中选择【卸载】。

3.4.6 安全终端 Linux 杀毒

3.4.6.1 字符界面卸载

第一步：以 Linux 超级用户身份登录到系统中；

第二步：如果使用安装光盘方式卸载，则进入到光盘中安全终端 Linux 杀毒安装包目录下，将安全终端 Linux 杀毒软件光盘正确加载到系统中，执行光盘上的卸载程序./ravunsetup text（参数 text）。如果直接卸载，请退到根目录下，执行安装目录下的/bin/ravunsetup text（参数 text）程序；

第三步：开始卸载程序，程序询问是否全部删除安装目录下的内容：

输入“d”，删除安装目录下的文件；

输入“q”，退出卸载程序。

```
*****************************************************************************
*                                                                           *
*                                                                           *
*                  RISING ANTIVIRUS UNINSTALL SOFTWARE                      *
*       COPYRIGHT FOR BEIJING RISING TECHNOLOGY CO.,LTD. 2015-2016          *
*                                                                           *
*****************************************************************************
Please input the item you want to do:
[ d ]  :  Delete RISING ANTIVIRUS files in directory ”/usr/rav/rising” ?
[ q ]  :  Exit the uninstall ?
```

图表 3-137

第四步：根据上一步骤的选项，程序询问是否删除安装目录中的文件，如需删除输入“y”，不删除输入“n”，输入“q”，退出卸载程序，回车继续卸载；

```
Please input the item you want to do:
[ d ]  :  Delete RISING ANTIVIRUS files in directory "/usr/rav" ?
[ q ]  :  Exit the uninstall ?
d
Stopping the running application ,please waiting...
File /usr/rav/lib/libravinstall.so may be created after installation,Delete it?
[y]--delete it,[n]--no deleting,[q]--exit
```

图表 3-138

第五步：程序继续卸载直到完成，并显示出提示信息。

```
delete file /usr/rav/virbak/00000159 ...
delete file /usr/rav/virbak/000001FF ...
delete file /usr/rav/virbak/00000112 ...
delete file /usr/rav/virbak/00000020 ...
```

图表 3-139

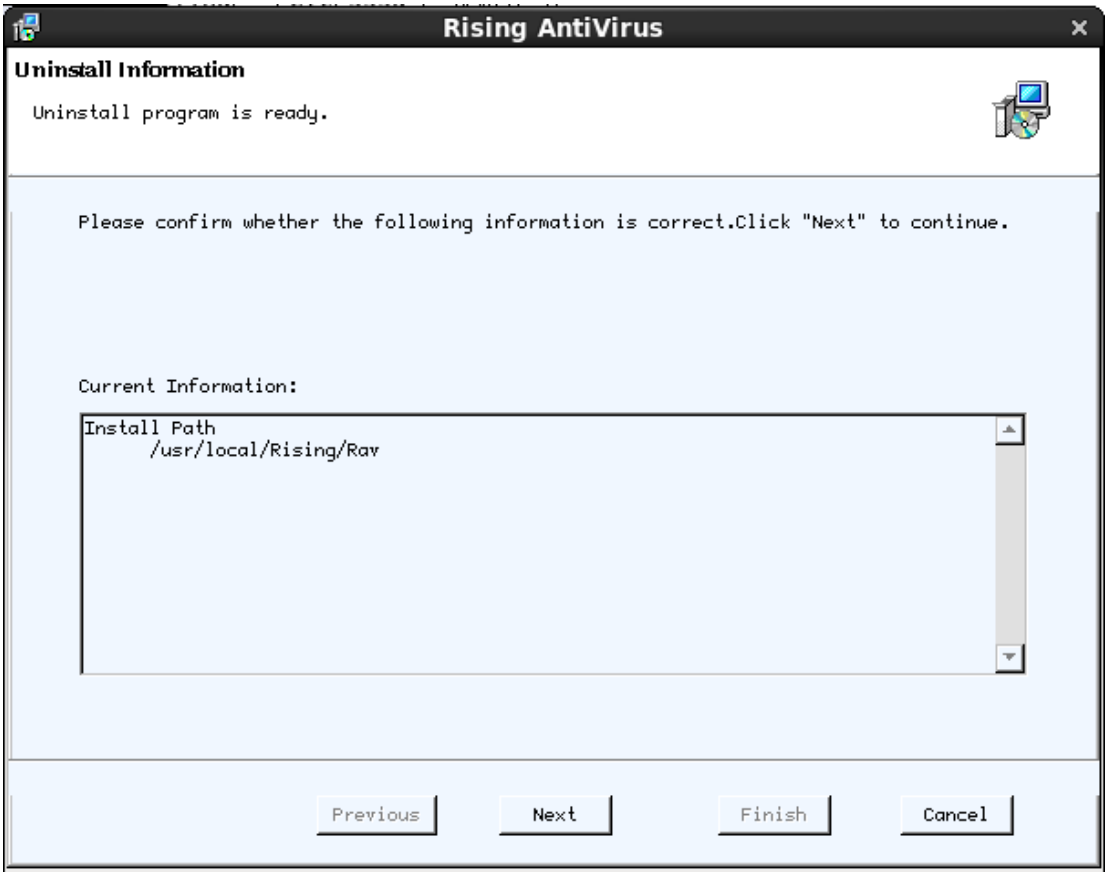
3.4.6.2 图形界面卸载

第一步：用 root 账户登录 Linux 系统。

第二步：打开终端，并在终端中运行命令：cd /，并进入到安全终端 Linux 杀毒安装包路径下。

第三步：运行瑞星卸载程序 ravunsetup；比如：安全终端 Linux 杀毒软件安装在

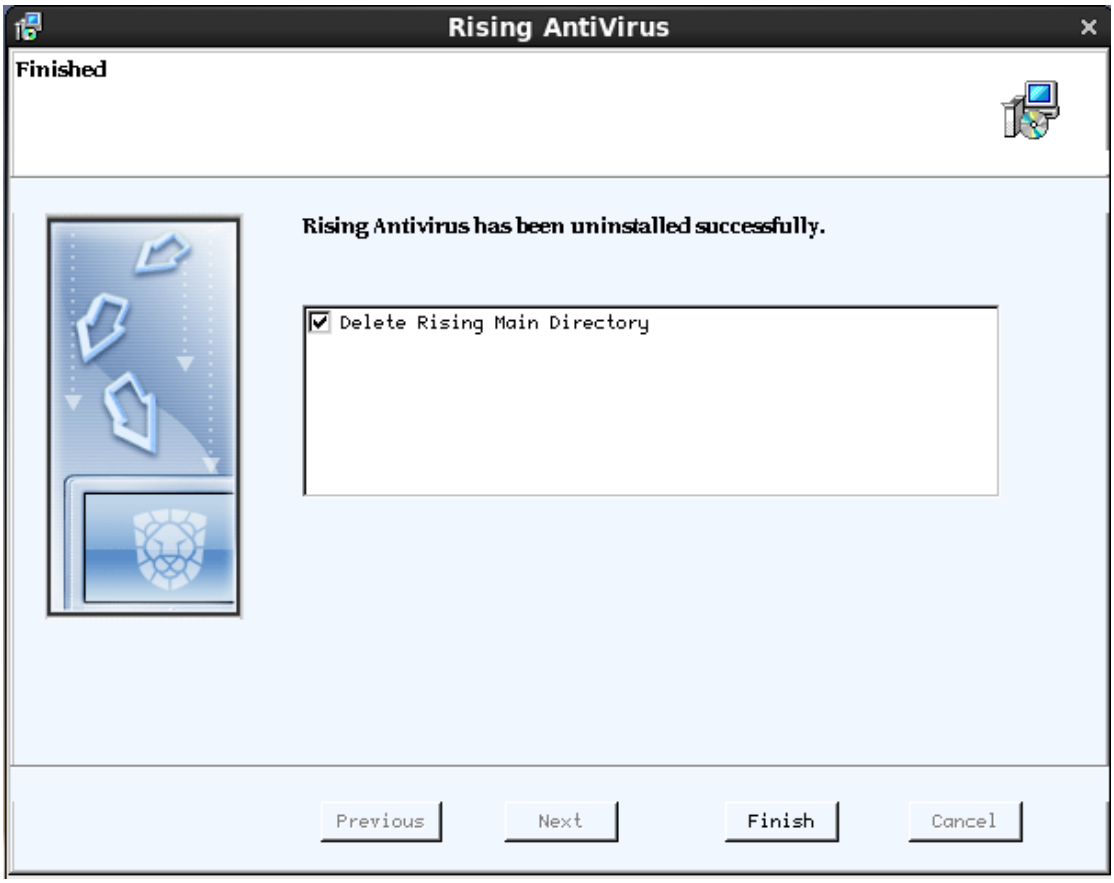
/usr/local/Rav 下，运行/usr/local/Rav/bin/ravunsetup。会出现卸载界面，点击【Next】。



图表 3-140

提示：如果界面提示“请使用root权限卸载！”说明尝试卸载软件的用户没有root权限，请先获得正确的权限，然后再进行卸载。建议直接使用root账户卸载。

第四步：卸载完成，确认是否需要保留文件目录，勾选表示删除安全终端 Linux 杀毒软件相关目录，不勾选表示保留，点击【Finish】。root 用户桌面的安全终端 Linux 杀毒软件快捷图标也将自动删除。



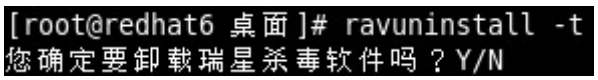
图表 3-141

3.4.7 Linux 全功能防护客户端

3.4.7.1 字符界面卸载

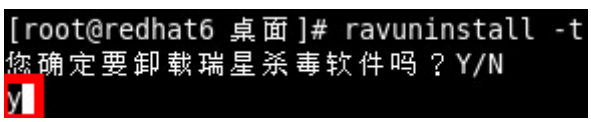
用户可在字符界面下通过 ravuninstall –t 命令来卸载瑞星杀毒软件 for Linux。

注意：卸载软件需要root权限。



图表 3-142

界面提示“您确定要卸载瑞星杀毒软件吗?Y/N”确认信息，输入“y”并按“回车”确认卸载。

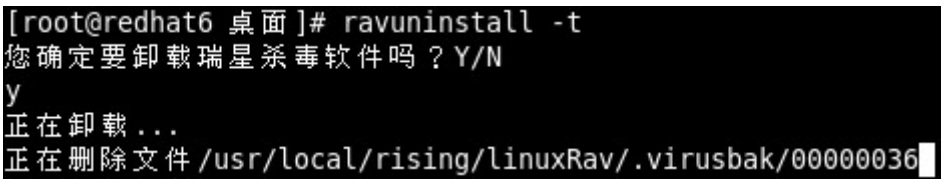


图表 3-143

注意：如果界面提示“请使用root权限卸载！”说明尝试卸载软件的用户没有root权限，请先获得正确的权限，然后再进行卸载。

图表 3-144

正常情况下，用户在确认卸载后，软件开始进行卸载，并提示正在卸载的文件信息。



图表 3-145

卸载结束后，软件提示“卸载完成，部分文件在系统重启后删除！”

图表 3-146

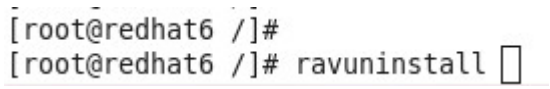
用户可重启系统完成卸载过程，至此在字符界面下卸载杀毒软件成功。

3.4.7.2 图形界面卸载

在安装瑞星杀毒软件后，用户可随时对其进行卸载。

注意：卸载软件需要root权限。

首先打开一个终端窗口，以 root 权限执行命令 ravuninstall



图表 3-147

在“你确定要卸载瑞星杀毒软件吗”窗口点击“卸载”按钮。

图表 3-148

如果显示“卸载失败，请用 root 权限卸载”说明正在卸载软件的用户没有 root 权限，请先获得权限，然后再次尝试卸载软件。

图表 3-149

如果权限正常，之后软件会显示卸载过程及进度。

图表 3-150

最后，软件提示重启系统，点击“立即重启”完成卸载。

图表 3-151

至此软件卸载成功。

4 安全管理

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

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终端安全状态的管理工具。管理员通过管理控制台，可以了解整个用户网络的总体安全状况，直观的查看所有终端当前的实时监控状态、病毒查杀情况、组件版本信息等；能够对任意终端执行远程安全管理，进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个用户网络中建立起坚实的安全防护系统。

图表 4-1

4.1.1 控制台

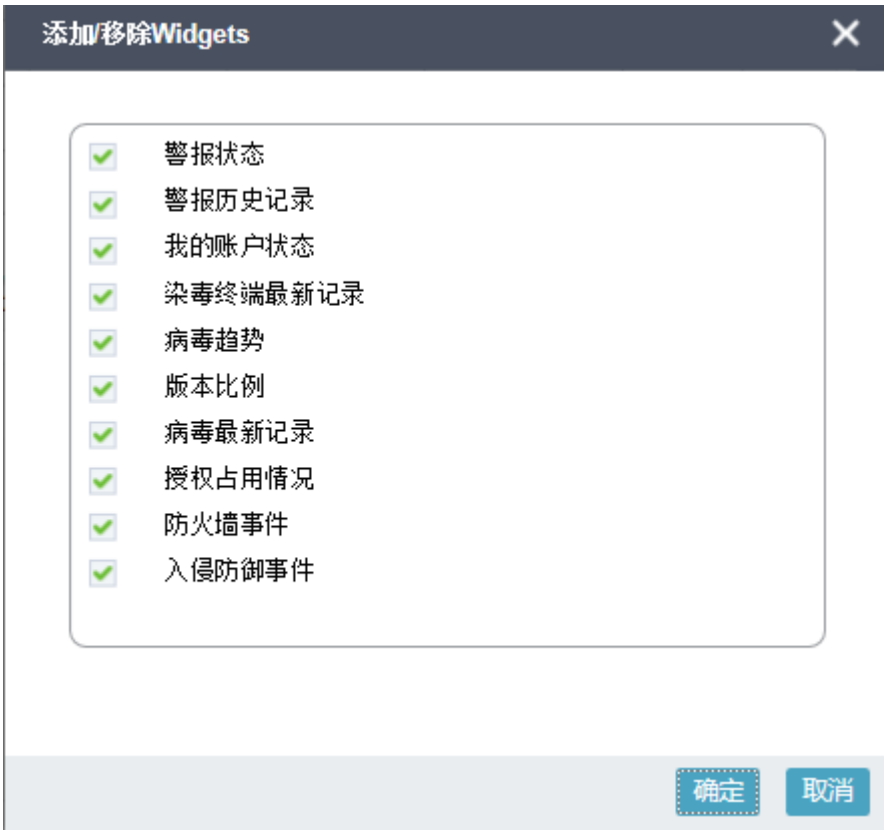
4.1.1.1 时间视图

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切换标签，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左上方的【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

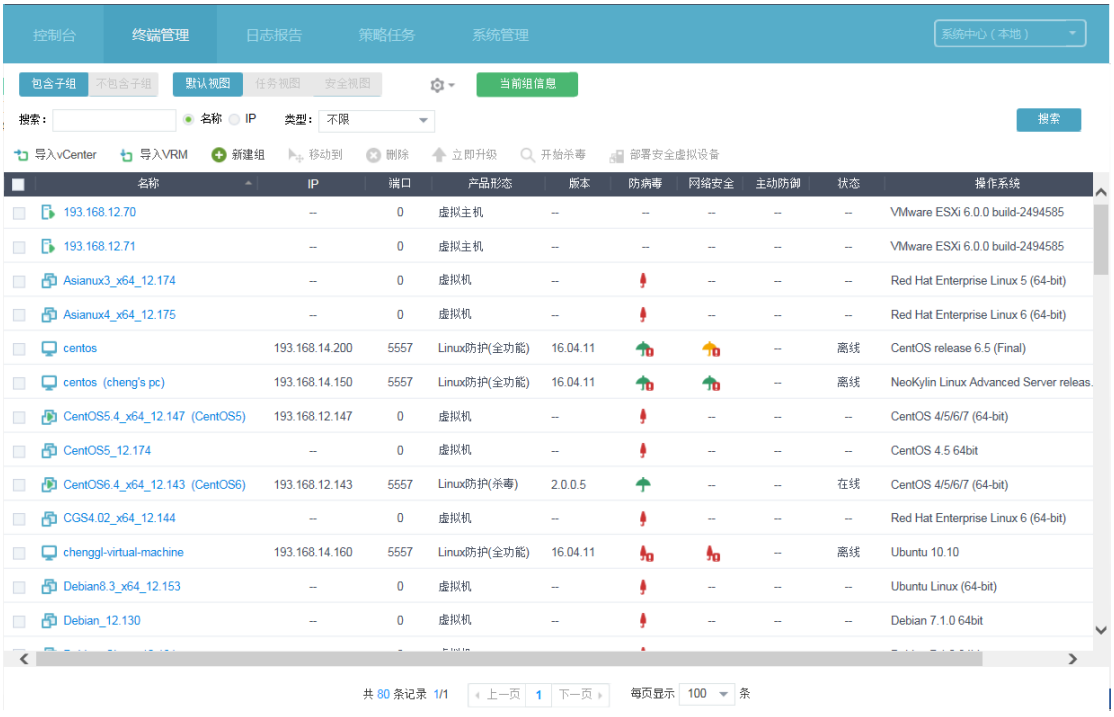
4.1.2 终端管理

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、产品形态、版本、防病毒、网络安全、主动防御、状态、操作系统和主机。

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 4-5

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 4-6

图中小伞图标表示防病毒、网络安全是否开启。小伞为绿色时表示全部监控开启，小伞为黄色时表示部分监控开启，小伞为红色时表示监控关闭，小伞带叹号表示未授权。

4.1.2.1 导入

4.1.2.1.1 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。

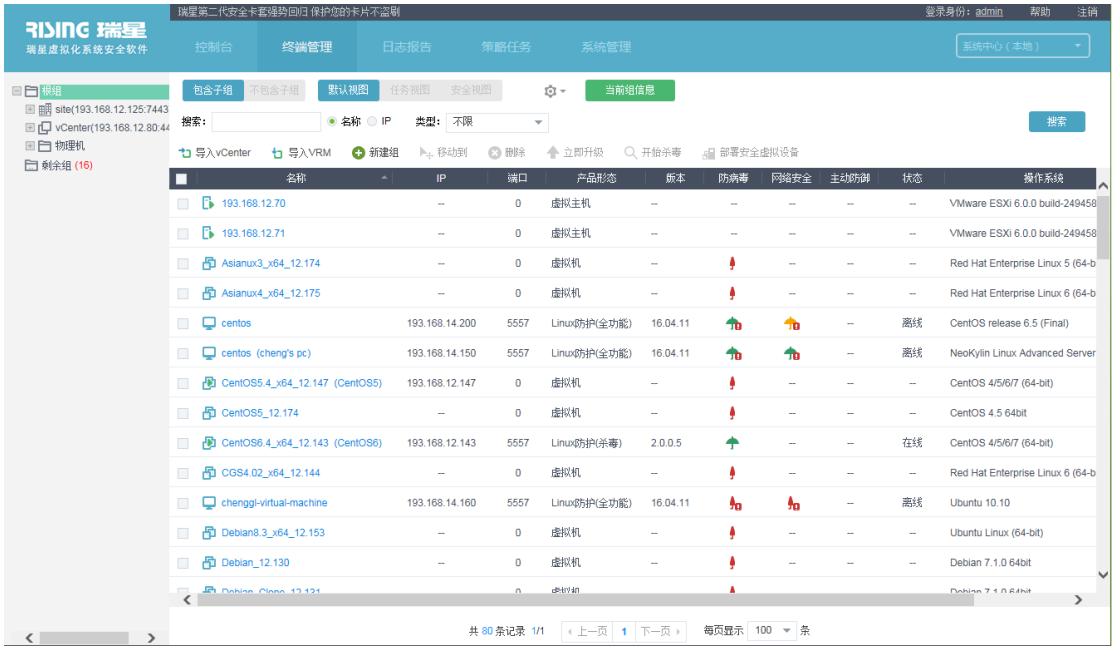
提示：初始用户名为admin，初始密码为123456。

图表 4-7

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 4-8

第三步：切换到【终端管理】标签页，点击工具栏的 导入vCenter 。

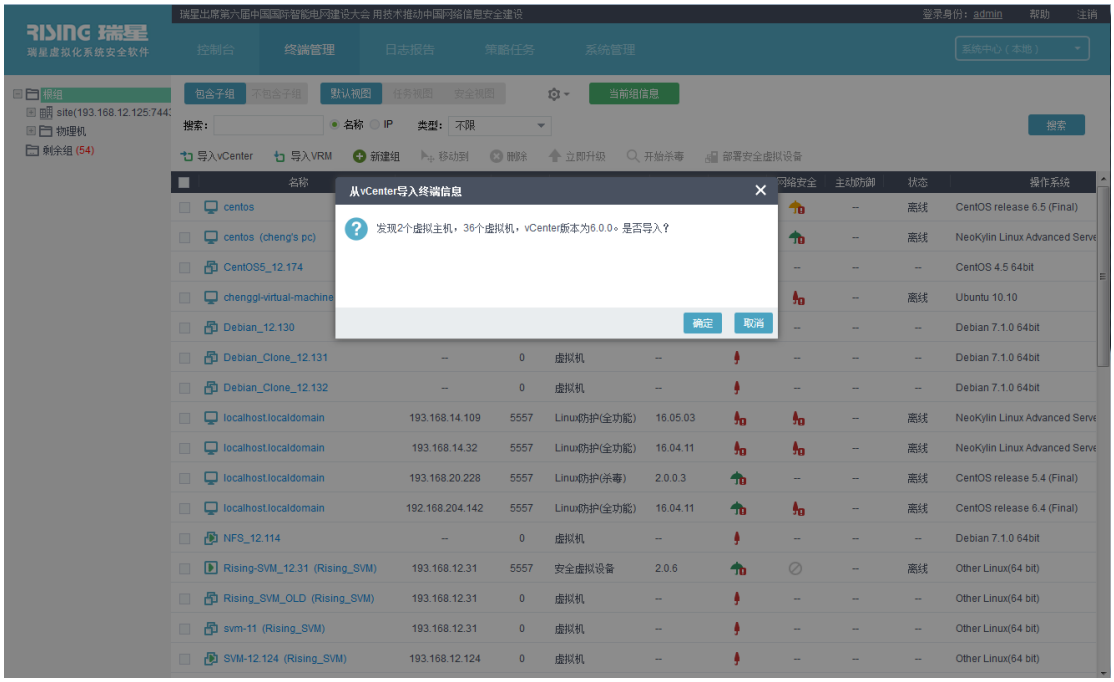


图表 4-9

第四步：在【从 vCenter 导入终端信息】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】。

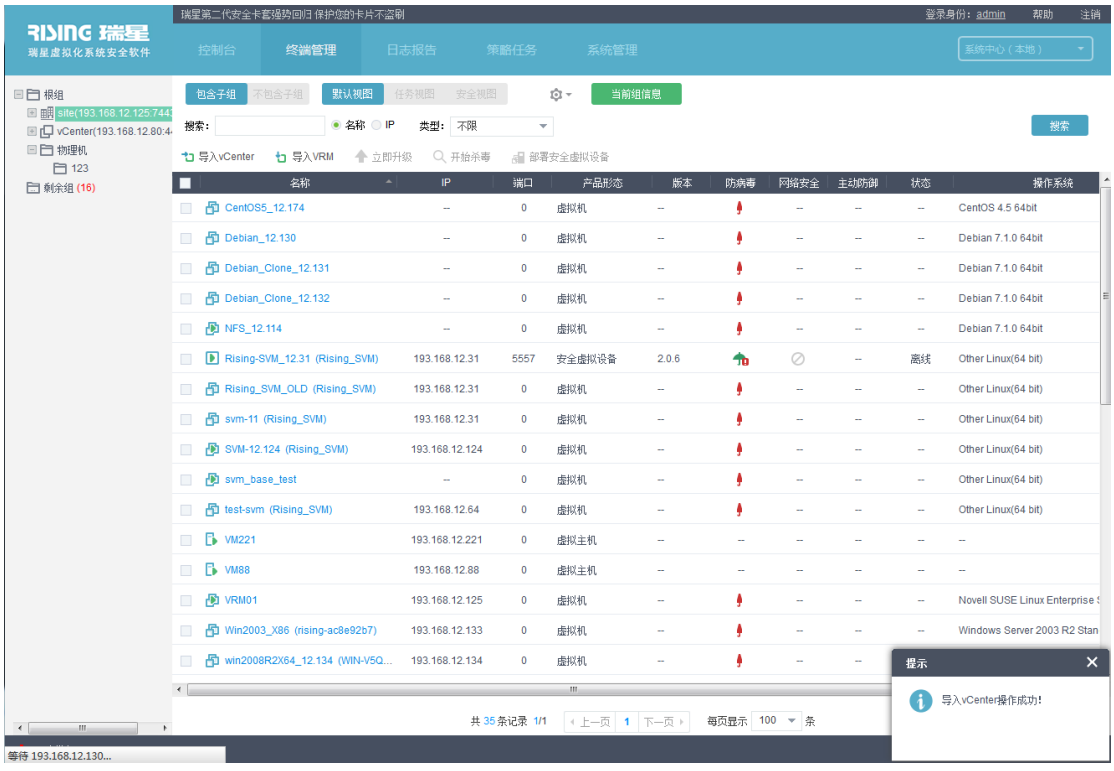
图表 4-10

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。



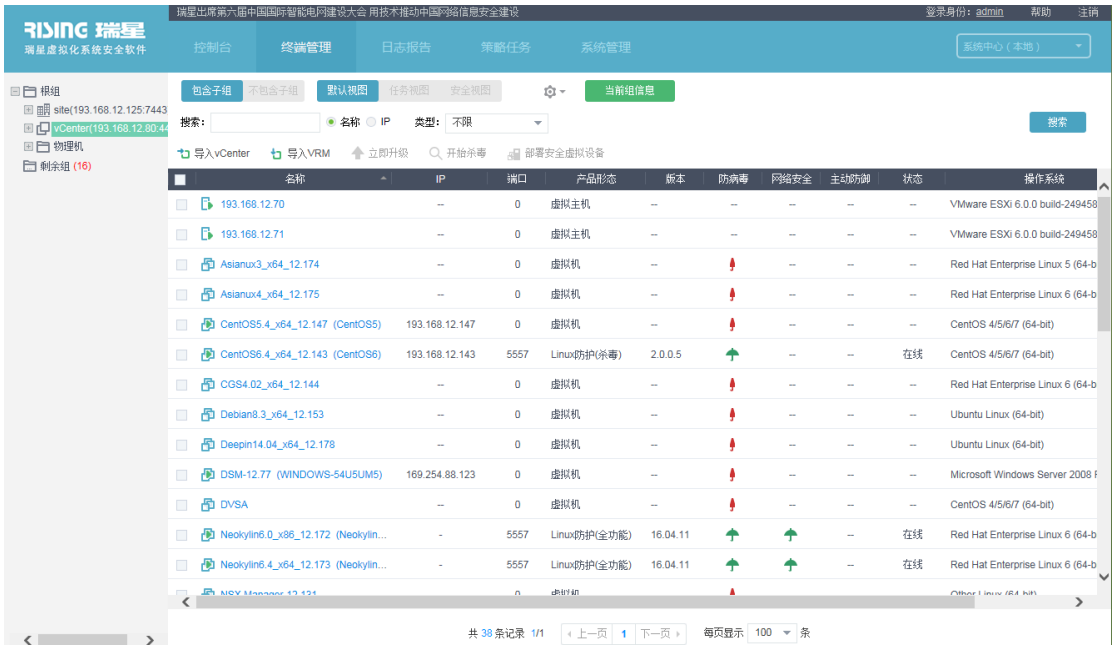
图表 4-11

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 4-12

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



图表 4-13

4.1.2.1.2 导入 VRM 终端

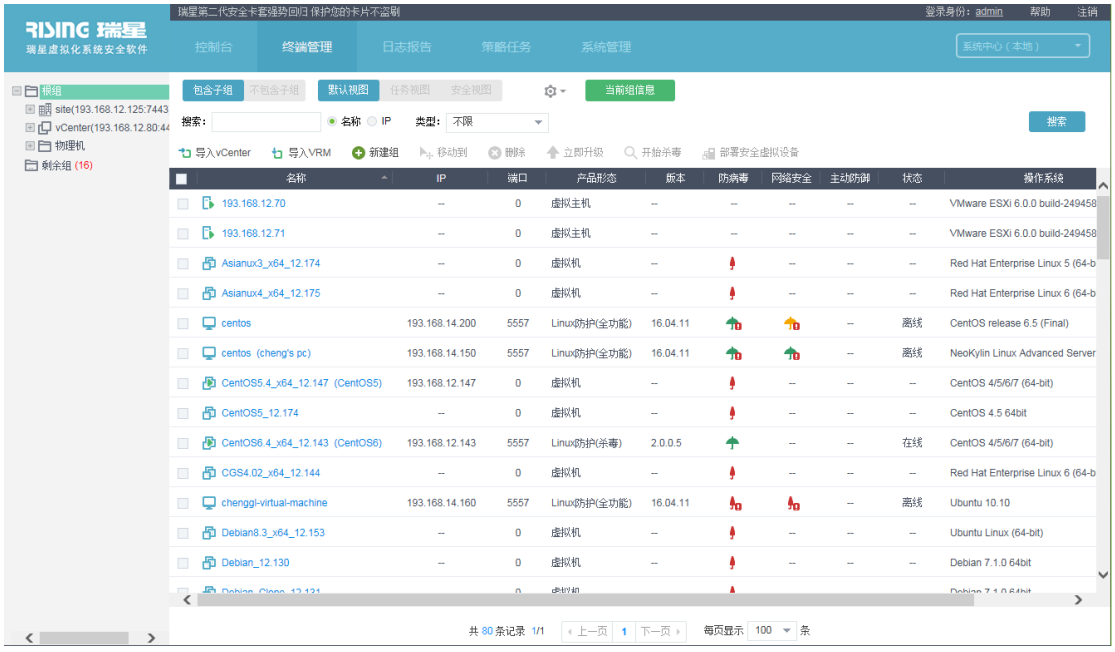
第一步：在浏览器中打开瑞星虚拟化系统安全软件管理中心服务器地址，输入用户名、密码，进行登录。

图表 4-14

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 4-15

第三步：切换到【终端管理】标签页，点击工具栏的 导入VRM 。

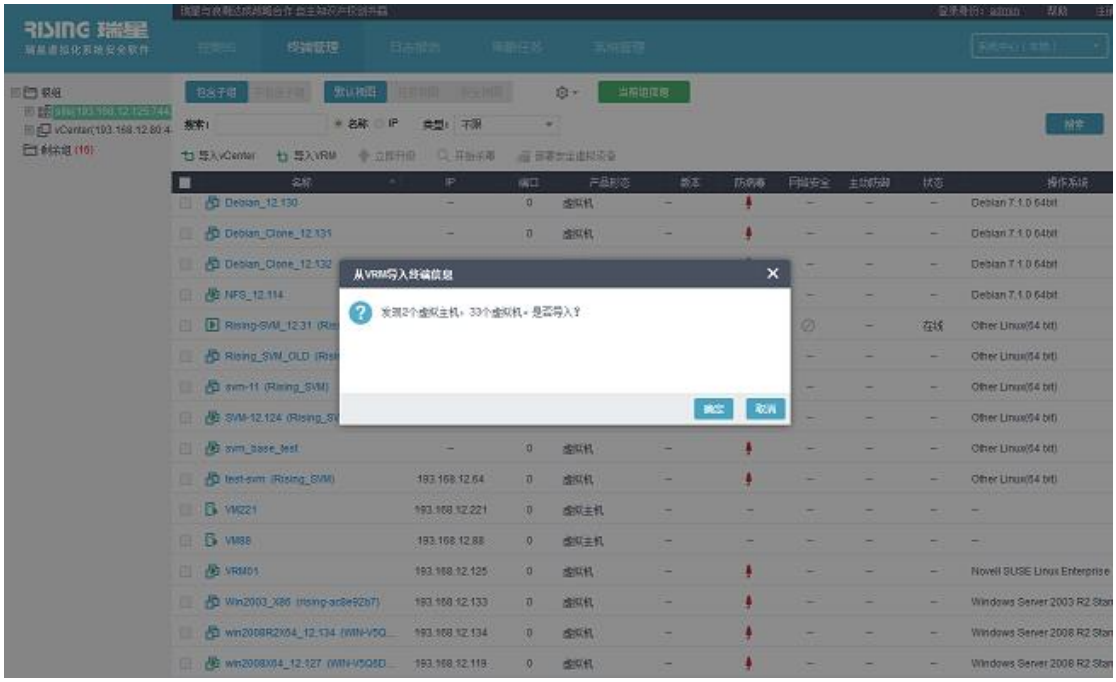


图表 4-16

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

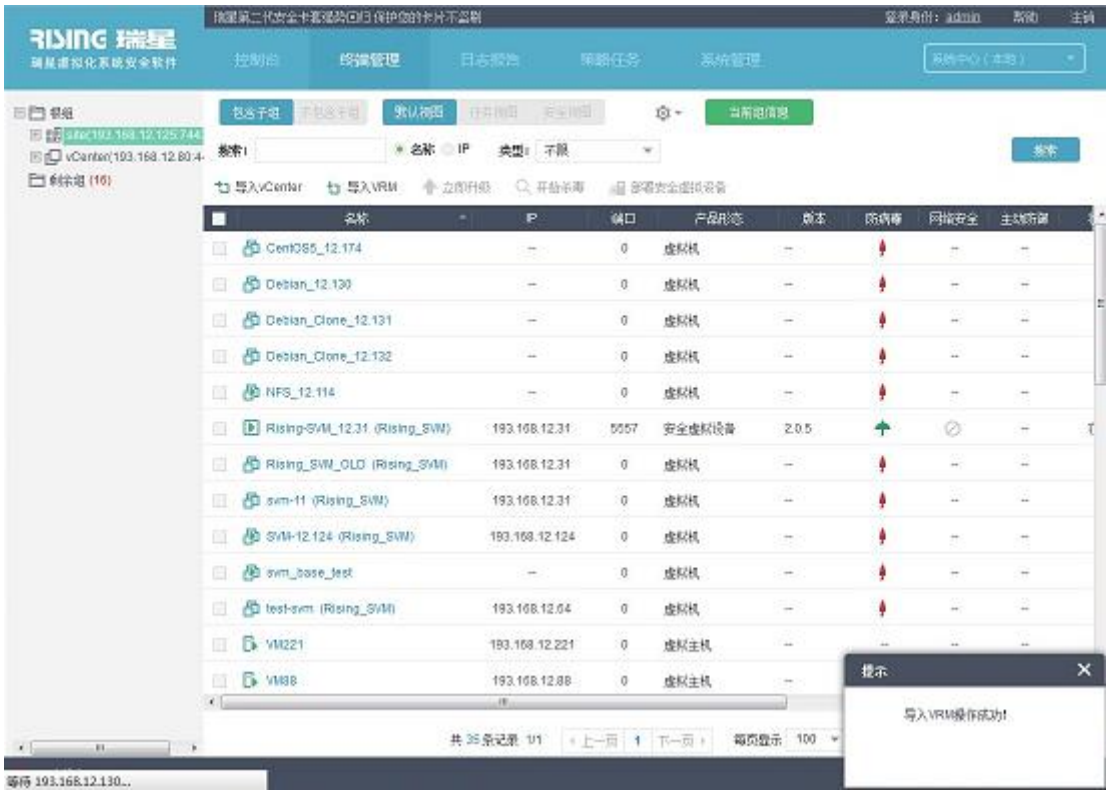
图表 4-17

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



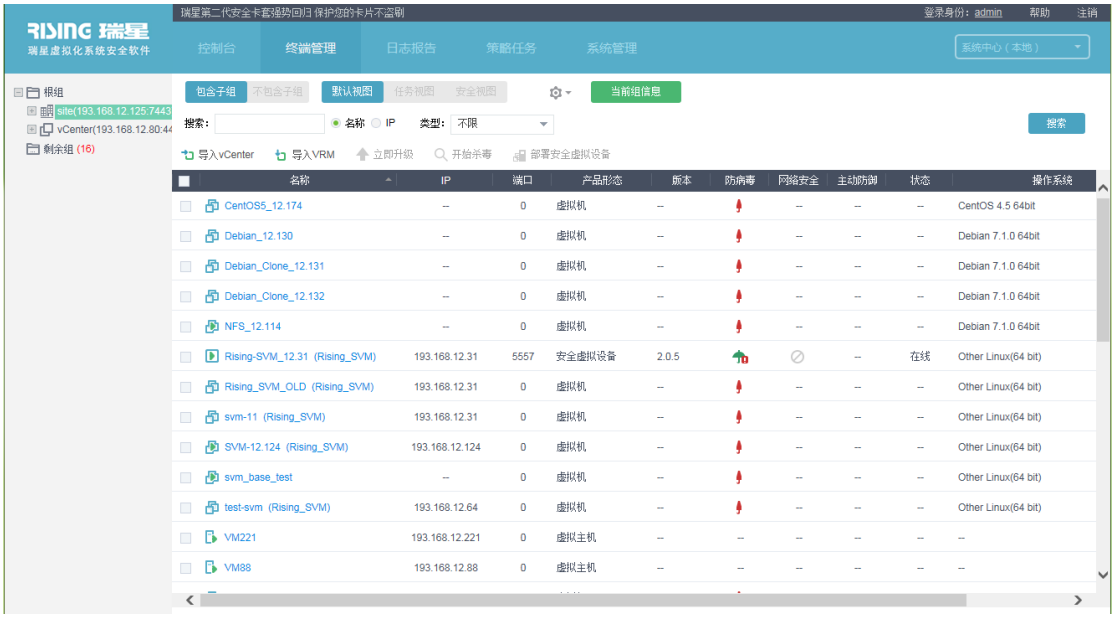
图表 4-18

第六步：确定导入后，右下角弹出窗口提示：“导入 VRM 操作成功”。



图表 4-19

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



图表 4-20

4.1.2.2 组

导航窗口显示的终端组分为：包括 vCenter 导入组、VRM 导入组、物理机组和剩余组。

4.1.2.2.1 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  ，可以对 vCenter 导入组执行刷新、删除、立即升级和开始杀毒操作。

图表 4-21

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 

、进行终端组件的升级、开始杀毒操作。

选中 vCenter 导入组，点击右上角 

，显示其详细信息，包括组信息、任务和日志信息。

组信息

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

生效。

图表 4-22

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 4.1.4.2 任务。

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 4.1.2.4.5 日志。

4.1.2.2.2 VRM 导入组

VRM 导入组信息从 VRM 获取，内部结构只读。点击右  ，可以对 VRM 导入组执行刷新、删除、立即升级和开始杀毒操作。

图表 4-23

VRM 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 

、 

、进行终端组件的升级、开始杀毒操作。

选中 VRM 导入组，点击右上角 

，显示其详细信息，包括组信息、任务和日志信息。

组信息

【组信息】显示基本信息和 VRM 信息。修改信息后，点击 

生效。

图表 4-24

任务

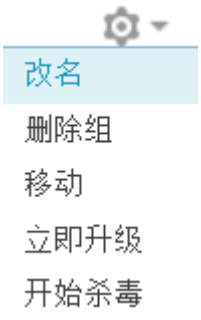
【任务】显示组相关任务状态，具体操作方法请参考本文档章节 4.1.4.2 任务。

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 4.1.2.4.5 日志。

4.1.2.2.3 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 ，可以对自定义组执行改名、删除、移动、立即升级和开始杀毒操作。



图表 4-25

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 、 开始杀毒 、进行终端组件的升级和开始杀毒。

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、任

务、策略设置和日志记录信息。

组信息

【组信息】显示基本信息。修改信息后，点击 保存 生效。

图表 4-26

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 4.1.2.4.3 任务。

策略设置

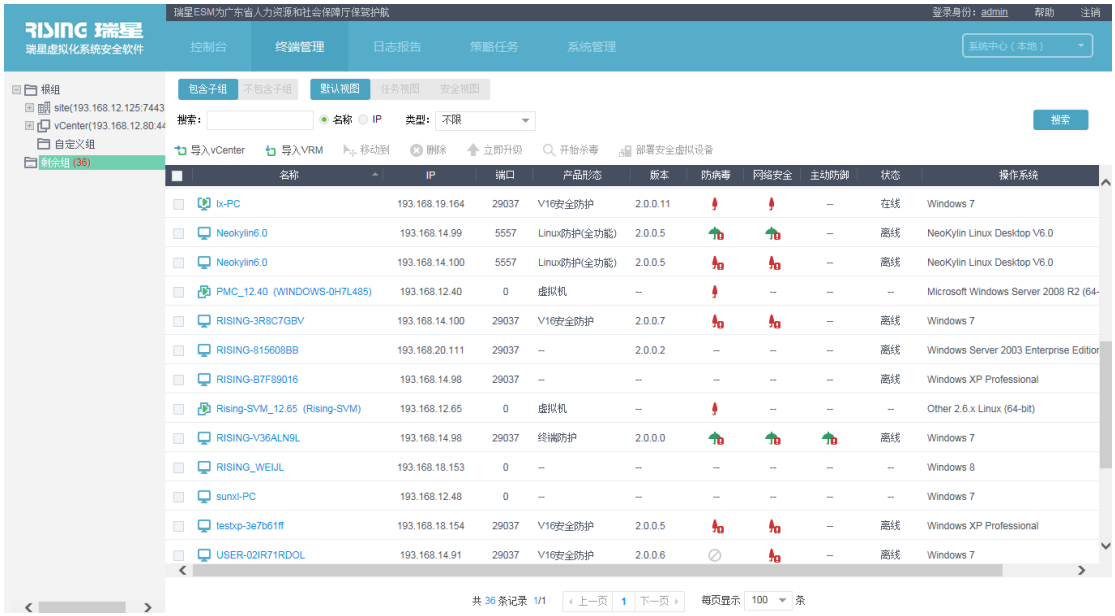
显示组相关策略设置，具体操作方法请参考本文档章节 4.1.2.4.4 策略设置。

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 4.1.2.4.5 日志。

4.1.2.2.4 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 RSTools 组件后的物理机将被自动发现并加入剩余组中。



图表 4-27

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 、 开始杀毒 、进行终端组件的升级和开始杀毒。

4.1.2.3 虚拟主机

点击【site】/【host】，或者点击【vCenter】/【DataCenter】/【host】，显示虚拟主机列表，点击虚拟主机列表中的虚拟主机名称，显示其详细信息。

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、软件版本及备注。可以修改备注，点击 保存 生效。

图表 4-28

4.1.2.4 安全虚拟设备

点击【site】/【vm】，或者点击【vCenter】/【DataCenter】/【vm】，显示虚拟机列表，点击虚拟机列表中的安全虚拟设备名称，显示其详细信息，包括终端信息、任务、策略设置和日志。

4.1.2.4.1 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。

【授权状态】显示安全虚拟设备授权状态。

图表 4-29

4.1.2.4.2 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 4.1.4.2 任务。

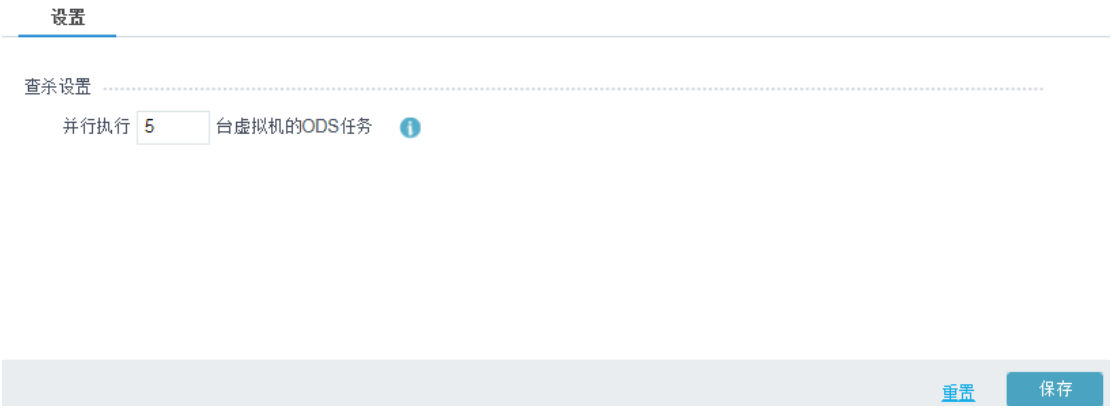
4.1.2.4.3 策略设置

【策略设置】分为【安全虚拟设备】和【升级与日志】。

4.1.2.4.3.1 安全虚拟设备

【查杀设置】

当选中批量终端同时进行杀毒时，用于设置该安全虚拟设备所在的虚拟主机上，允许同时执行杀毒的终端的数量。超出该数值的终端，不会进行杀毒，而是排队等待，当有终端杀毒完毕后，再从队列中排队等待的终端中调度对应的数量进行补充，执行杀毒处理。该设置能够避免批量终端集中查杀时，导致的虚拟主机资源风暴。



图表 4-30

4.1.2.4.3.2 升级与日志

【升级】显示安全虚拟设备升级策略信息。

定时设置

配置定时升级的启用状态和开始时间。

图表 4-31

升级方式设置

配置升级源地址。

图表 4-32

网络连接设置

配置网络连接方式。

图表 4-33

【日志】显示安全虚拟设备日志策略信息。

日志中心

配置日志中心地址。

图表 4-34

4.1.2.4.4 日志

【日志】主要显示安全虚拟设备的【事件日志】，具体操作方法请参考本文档章节 4.1.3.1.1 事件日志。

4.1.2.5 终端

点击终端名称，显示其详细信息，包括包括终端信息、任务、策略设置、日志和升级中心版本。

4.1.2.5.1 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、软件版本及备注。点击立即升级，可以执行虚拟机 RSTools 组件升级操作，还可以修改备注信息，点击 保存 生效。

图表 4-35

4.1.2.5.2 任务

【任务】显示虚拟机相关任务状态，具体操作方法请参考本文档章节 4.1.4.2 任务。

4.1.2.5.3 策略设置

【策略设置】主要为 VMware 无代理杀毒、HUAWEI 无代理杀毒、安全防护终端、全功能安全防护客户端、安全终端 Linux 杀毒和 Linux 全功能防护客户端进行策略设置。

VMware 无代理杀毒的策略设置包括【杀毒（VMware）】。

HUAWEI 无代理杀毒的策略设置包括【杀毒（Huawei）】、【防火墙（Huawei）】、【IP 黑白名单（Huawei）】、【入侵防御（Huawei）】和【WEB 信誉（Huawei）】。

安全防护终端的策略设置包括【杀毒（Windows）】、【防火墙（Windows）】、【主动防御（Windows）】。

全功能安全防护客户端的策略设置包括【公共】、【杀毒】和【防火墙】。

安全终端 Linux 杀毒的策略设置包括【杀毒（Linux）】。

Linux 全功能防护客户端的策略设置包括【杀毒&防火墙（Linux）】。

4.1.2.5.3.1 杀毒（VMware）

【杀毒（VMware）】显示 VMware 虚拟机相关的杀毒策略信息，包括扫描和文件监控，具体操作方法请参考本文档章节 4.1.4.1 策略模板部分。

4.1.2.5.3.2 杀毒（Huawei）

【杀毒（Huawei）】显示 Huawei 虚拟机相关的杀毒策略信息，包括扫描和文件监控，具体操作方法请参考本文档章节 4.1.4.1 策略模板部分。

4.1.2.5.3.3 防火墙（Huawei）

【防火墙（Huawei）】显示 Huawei 虚拟机相关的防火墙策略信息，包括启用防火墙功能。

图表 4-36

4.1.2.5.3.4 IP 黑白名单（Huawei）

【IP 黑白名单（Huawei）】显示 Huawei 虚拟机相关的 IP 黑白名单策略信息，包括启用自定义 IP 黑名单、拦截时记录日志、启用自定义 IP 白名单和记录日志。

IP 黑名单

图表 4-37

IP 白名单

图表 4-38

4.1.2.5.3.5 入侵防御（Huawei）

【入侵防御（Huawei）】显示 Huawei 虚拟机相关的入侵防御策略信息，包括 IDS/IPS 专家规则库、SQL 防注入专家规则库和是否记录日志。

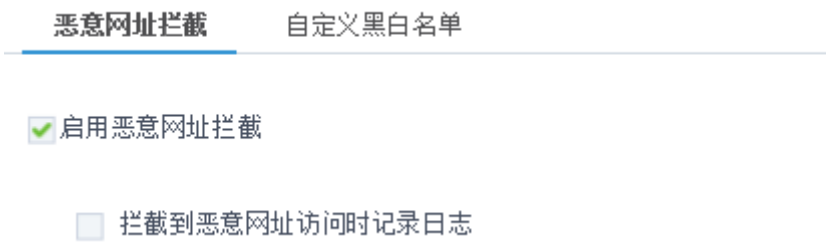
IDS/IPS

图表 4-39

4.1.2.5.3.6 WEB 信誉（Huawei）

【WEB 信誉（Huawei）】显示 Huawei 虚拟机相关的 WEB 信誉策略信息，包括启用恶意网址拦截、拦截到恶意网址访问时记录日志、HTTP 黑名单、拦截时记录日志和 HTTP 白名单。

恶意网址拦截



图表 4-40

自定义黑白名单

图表 4-41

4.1.2.5.3.7 VPatch（Huawei）

【VPatch】显示 Huawei 虚拟机相关的的 VPatch 策略信息，包括启用 VPatch 专家规则库和是否记录日志等。

图表 4-42

4.1.2.5.3.8 杀毒（Windows）

【杀毒（Windows）】显示安全防护终端相关的杀毒策略信息，包括手动扫描、定时扫描、文件监控和其它策略信息。

手动扫描

配置文件类型过滤选项、扫描类型设置、优化选项、发现病毒时处理、杀毒失败时处理、杀毒结束后处理隔离失败时处理和查杀目标。

图表 4-43

图表 4-44

图表 4-45

定时扫描

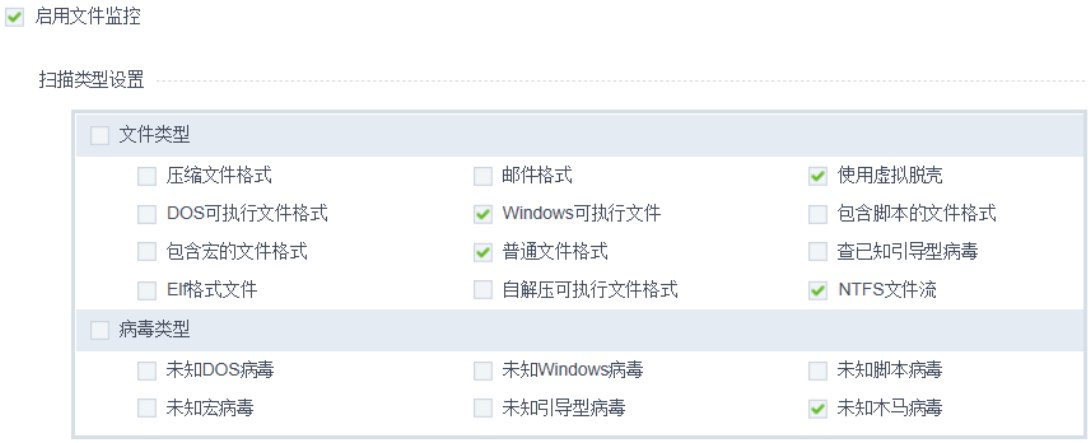
配置文件类型过滤选项、扫描类型设置、优化选项、发现病毒时处理、杀毒失败时处理、杀毒结束后处理、隔离失败时处理和查杀目标。

图表 4-46

文件监控

配置文件监控的启用、扫描类型设置、优化选项、发现病毒时处理、杀毒失败时处理、

备份失败时处理和其他设置。



图表 4-47

图表 4-48

其他设置

配置引擎设置和其他相关设置。

图表 4-49

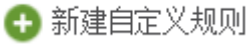
4.1.2.5.3.9 防火墙（Windows）

【防火墙（Windows）】显示安全防护终端相关的防火墙策略信息，包括 IP 包过滤、网络攻击拦截、恶意网址拦截、出站攻击防御和应用程序网络访问监控。

IP 包过滤

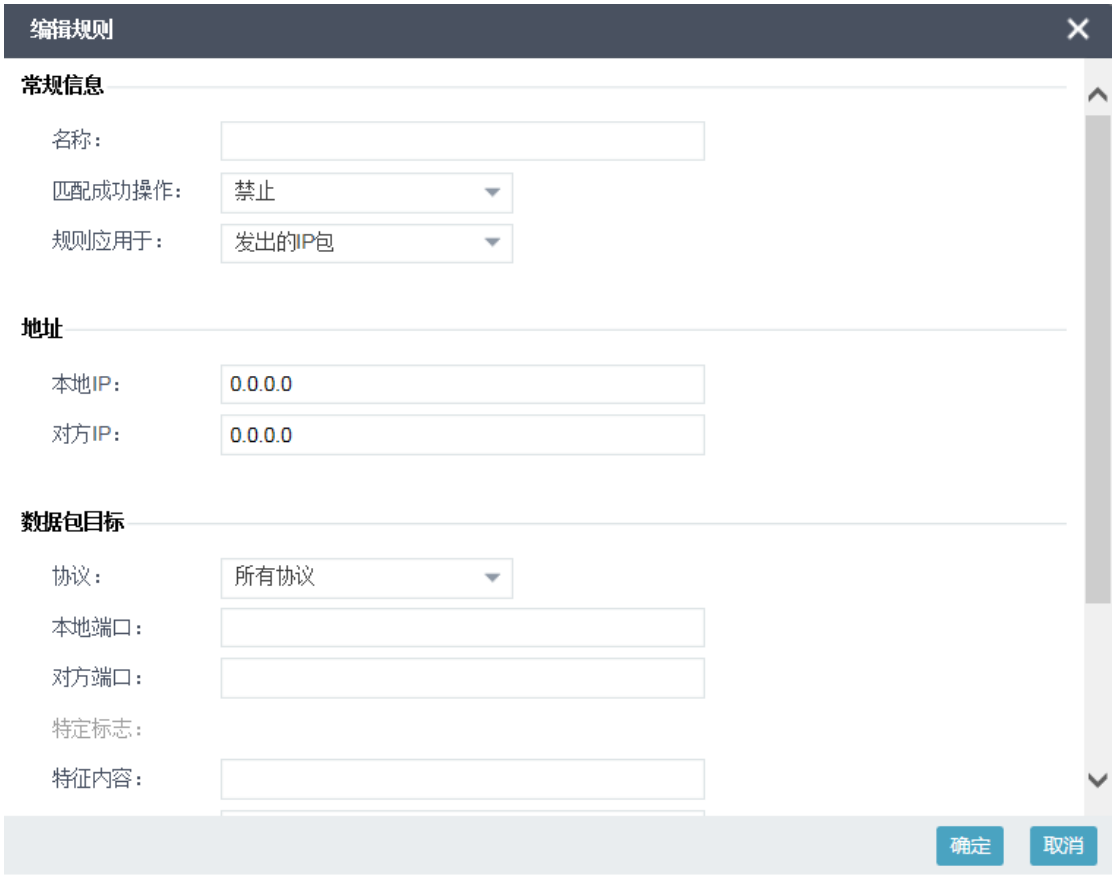
配置启用 IP 包过滤和新建自定义规则。

图表 4-50

点击 

，可以新建自定义规则，包括常规信息、地址、数据包目标和匹配成功后的报警方式，点击 

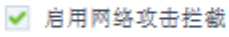
生效。



图表 4-51

网络攻击拦截

配置启用网络攻击拦截。



图表 4-52

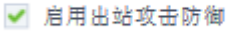
恶意网址拦截

配置启用恶意网址拦截。

图表 4-53

出站攻击防御

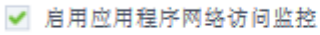
配置启用出站攻击防御



图表 4-54

应用程序网络访问监控

配置启用应用程序网络访问监控。



图表 4-55

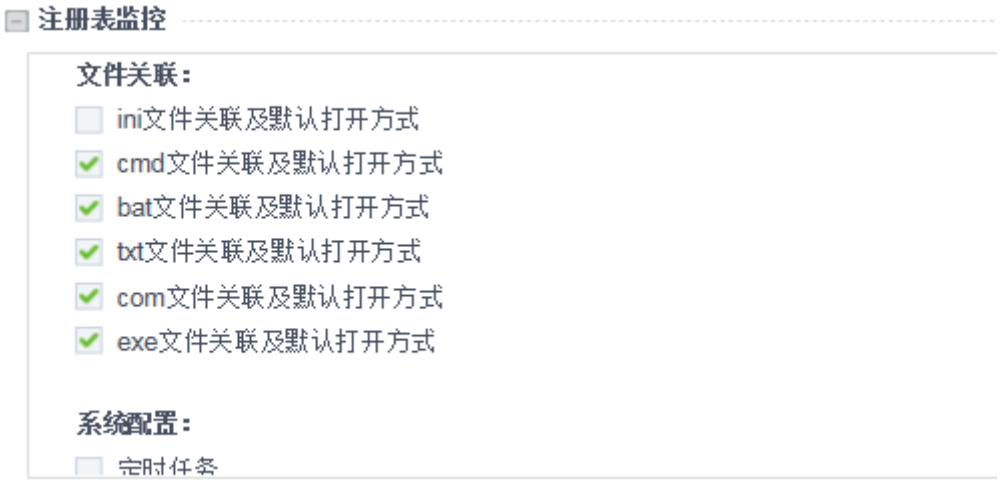
4.1.2.5.3.10 主动防御（Windows）

【主动防御（Windows）】显示安全防护终端相关的主动防御策略信息，包括系统加固、应用程序控制、木马行为防御、U 盘拦截、网站拦截、自我保护和自定义白名单。

系统加固

配置启用系统加固、系统动作监控、注册表监控、关键进程保护和系统文件保护，并可以勾选记录日志和开机时启用此功能。

图表 4-56


注册表监控
文件关联：
ini文件关联及默认打开方式
cmd文件关联及默认打开方式
bat文件关联及默认打开方式
txt文件关联及默认打开方式
com文件关联及默认打开方式
exe文件关联及默认打开方式
系统配置：

图表 4-57


关键进程保护
IE 浏览器控制：
cmd.exe
command.com
wscript.exe
csript.exe
其它应用程序
系统进程保护：
services.exe
winlogon.exe

图表 4-58


系统文件保护
系统关键目录：
电脑的组策略关机脚本
电脑的组策略启动脚本
电脑的组策略注销脚本
电脑的组策略登录脚本
系统目录
系统驱动文件目录
已下载程序目录
IE 浏览器目录
记录日志
开机时启用此功能

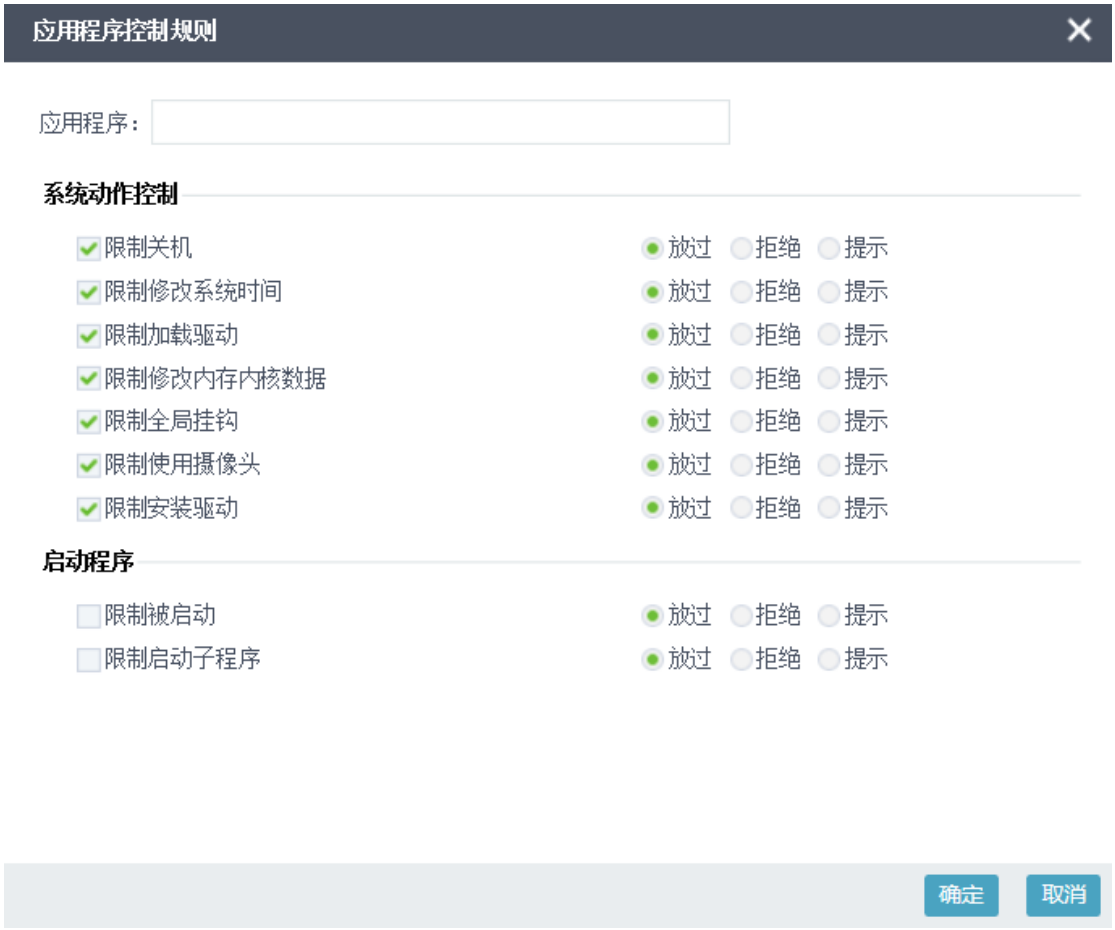
图表 4-59

应用程序控制

配置启用应用程序控制和添加规则，并可以勾选记录日志和开机时启用此功能。

图表 4-60

点击 添加规则，可以添加应用程序控制规则，包括应用程序名称、系统动作控制和限制启动程序，点击 确定 生效。



图表 4-61

木马行为防御

配置启用木马行为防御。

图表 4-62

U 盘拦截

配置启用 U 盘拦截、监控范围、发现程序在监控区域执行时处理、移动存储设备接入扫描和移动存储免疫，并可以勾选记录日志和开机时启用此功能。

图表 4-63

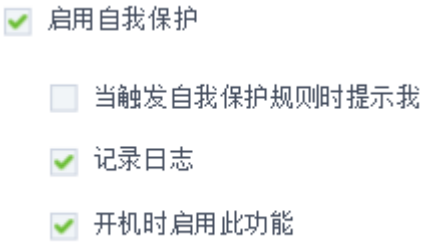
网站拦截

配置启用网站拦截、防御方式和发现网页病毒或危险脚本时处理，并可以勾选记录日志和开机时启用此功能。

图表 4-64

自我保护

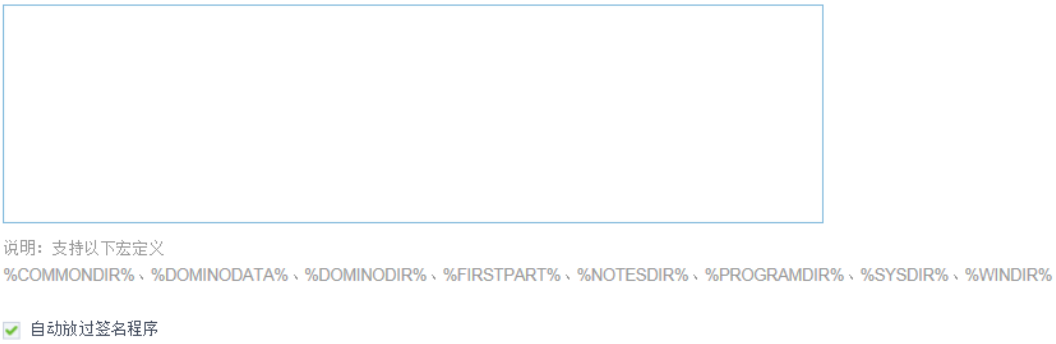
配置启用自我保护。



图表 4-65

自定义白名单

配置白名单，并可以勾选自动放过签名程序。



图表 4-66

4.1.2.5.3.11 公共

【公共】显示全功能安全防护客户端相关的公共策略信息，包括自我保护、云安全设置、扫描白名单和客户端密码。

自我保护

配置启用自我保护功能。

云安全设置

配置启用云安全功能。

扫描白名单

配置启用扫描白名单和添加扫描白名单功能。

客户端密码

配置启用客户端密码功能。

图表 4-67

4.1.2.5.3.12 杀毒

【杀毒】显示全功能安全防护客户端相关的杀毒策略信息，包括扫描、监控和完整性监控等策略信息。

4.1.2.5.3.12.1 扫描

【扫描】显示安全防护相关的扫描策略信息，包括设置、文件类型、病毒处理、扫描计划。

设置

配置启用流行病毒库查杀功能、启用智能启发式扫描、启用变频杀毒、扫描压缩包。

文件类型

配置扫描文件的类型。

病毒处理

配置发现恶意程序时处理方式。

扫描计划

配置启用定时扫描任务。

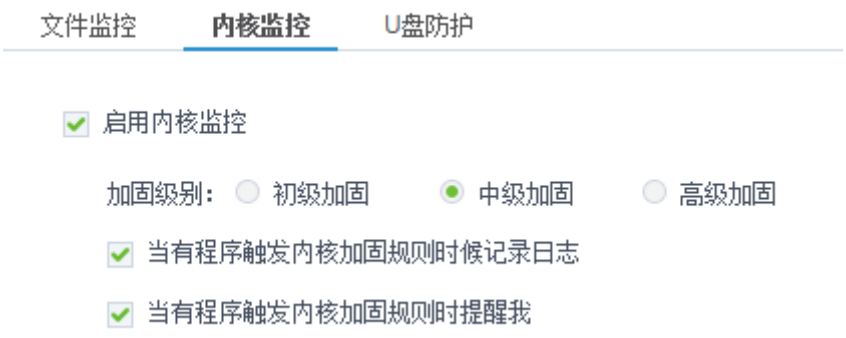
图表 4-68

4.1.2.5.3.12.2 监控

【文件监控】包括启用文件监控、监控等级、文件类型、优化选项和病毒处理设置等。

图表 4-69

【内核监控】包括启用内核监控和设置加固级别等。



图表 4-70

【U 盘防护】包括启用 U 盘防护、U 盘接入时自动进行安全扫描、阻止 U 盘上的程序自动执行和阻止 U 盘上的可执行程序执行等。

图表 4-71

4.1.2.5.3.12.3 完整性监控

【完整性监控】显示安全防护相关的完整性监控策略信息，包括文件访问和注册表访问。

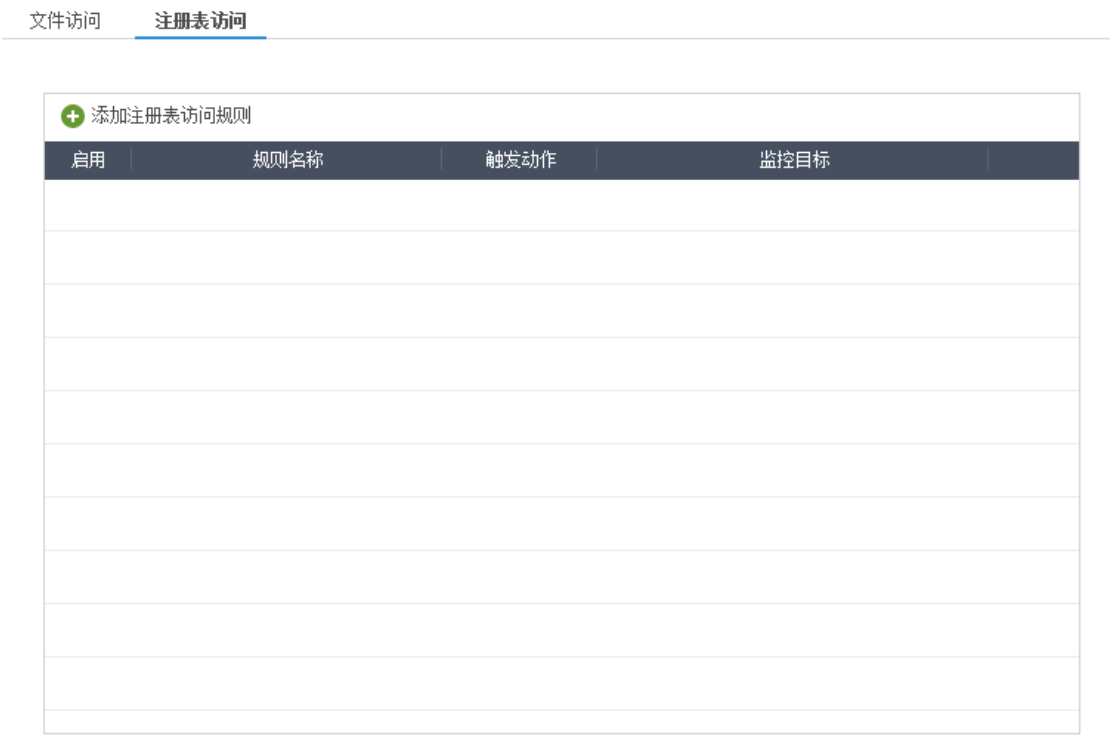
文件访问

添加文件访问规则。

图表 4-72

注册表访问

添加注册表访问规则。



图表 4-73

4.1.2.5.3.13 防火墙

【防火墙】显示全功能安全防护客户端相关的防火墙策略信息，包括 IP 规则、端口规则、IDS/IPS、VPatch、应用程序访问控制、阻止对外攻击、WEB 信誉、敏感词审查、上网管理和其他策略。

4.1.2.5.3.13.1 IP 规则

【IP 规则】显示 v16 安全防护相关的 IP 规则策略信息，包括 IP 规则、白名单和黑名单等。

IP 规则

配置启用 IP 规则、添加 IP 规则。

图表 4-74

白名单

配置添加白名单。

图表 4-75

黑名单

配置添加黑名单。

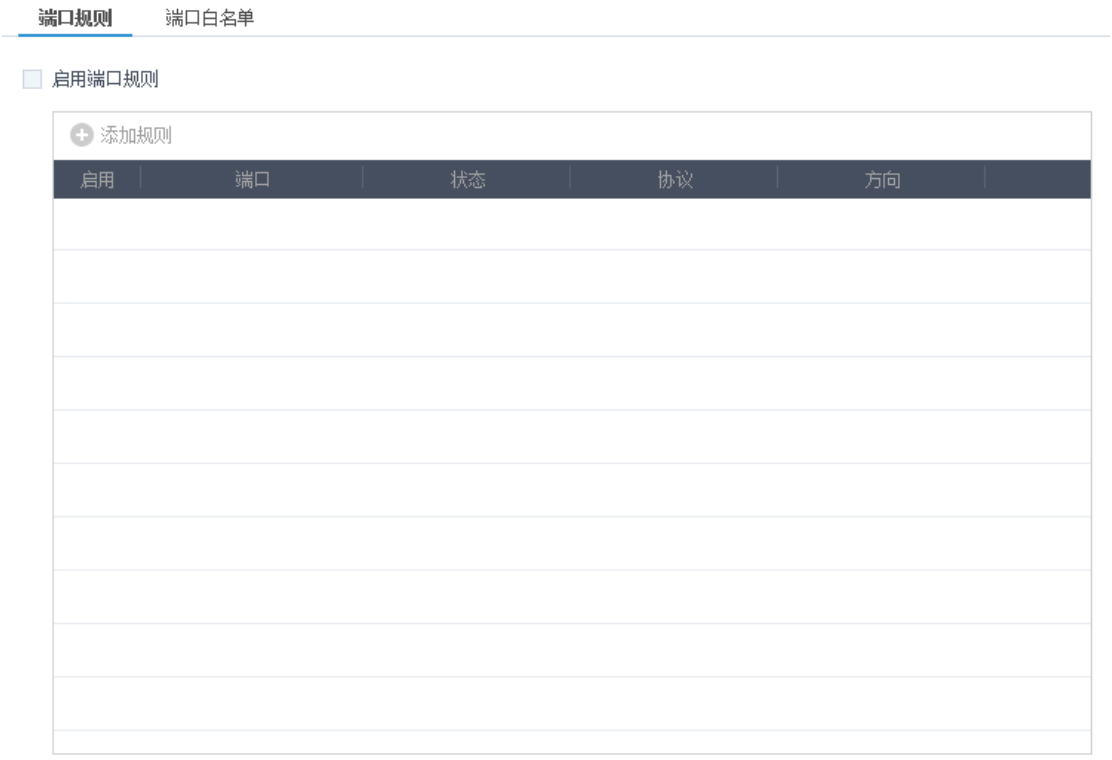
图表 4-76

4.1.2.5.3.13.2 端口规则

【端口规则】显示 v16 安全防护相关的端口规则策略信息，包括端口规则和端口白名单等。

端口规则

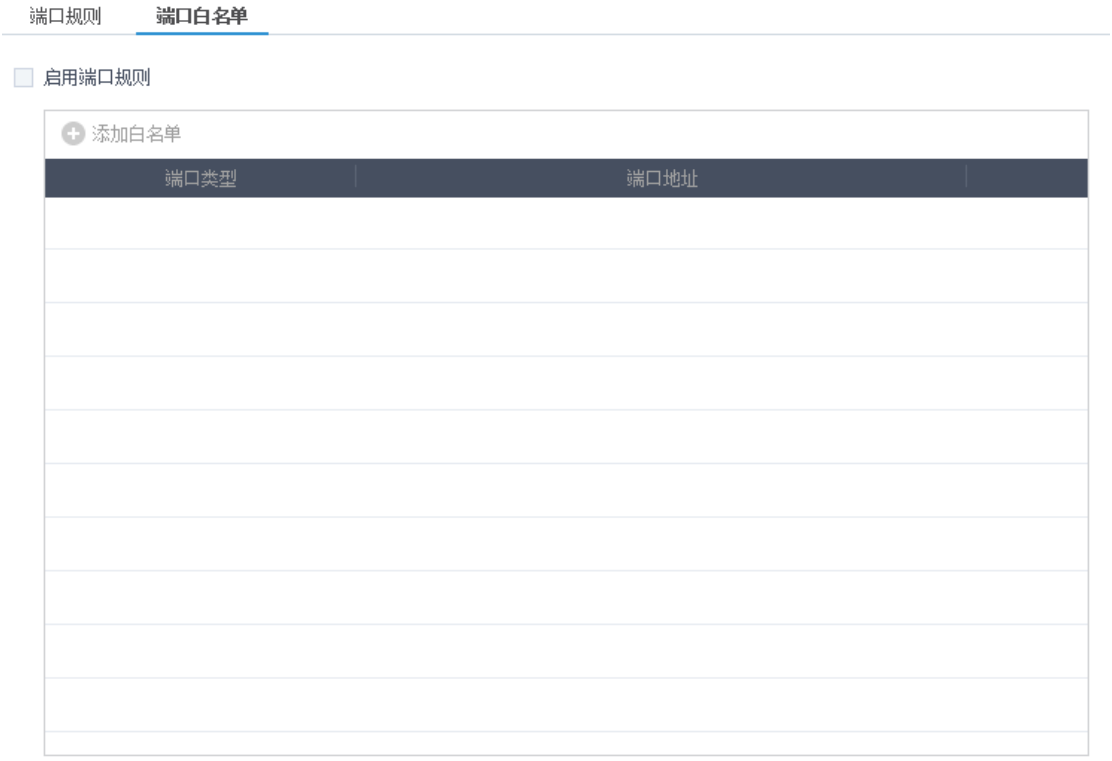
配置启用端口规则、添加规则。



图表 4-77

端口白名单

配置添加白名单。



图表 4-78

4.1.2.5.3.13.3 IDS/IPS

【IDS/IPS】显示 v16 安全防护相关的 IDS/IPS 策略信息，包括启用 IDS/IPS 规则、IDS/IPS 专家规则库和 SQL 防注入专家规则库等。

图表 4-79

4.1.2.5.3.13.4 VPatch

【VPatch】显示 v16 安全防护相关的 VPatch 策略信息，包括启用 VPatch 规则、VPatch 专家规则库、报警方式和是否记录日志等。

图表 4-80

4.1.2.5.3.13.5 应用程序访问控制

【应用程序访问控制】显示 v16 安全防护相关的应用程序访问控制策略信息，包括启用应用程序访问控制等。

图表 4-81

4.1.2.5.3.13.6 阻止对外攻击

【阻止对外攻击】显示 v16 安全防护相关的阻止对外攻击策略信息，包括启用阻止对外攻击、阻止对外攻击、报警方式和是否记录日志等。

图表 4-82

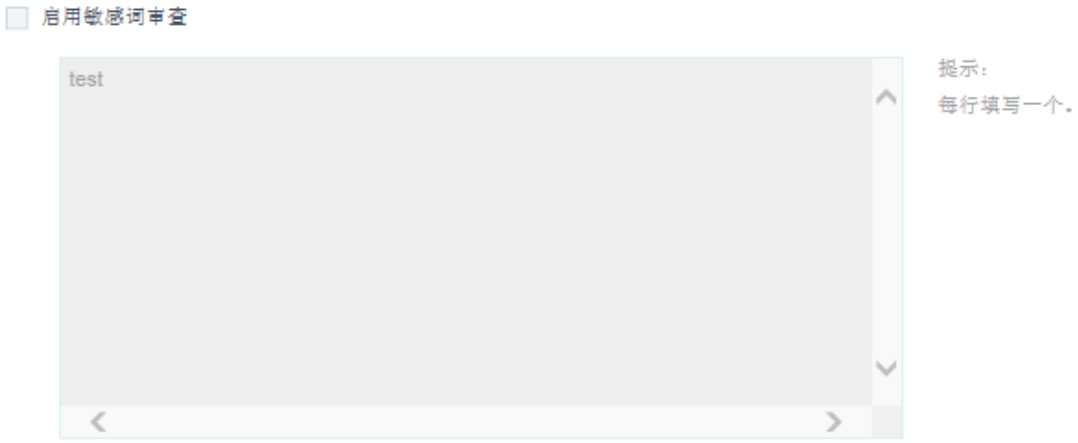
4.1.2.5.3.13.7 WEB 信誉

【WEB 信誉】显示 v16 安全防护相关的 WEB 信誉策略信息，包括启用 WEB 信誉、浏览器进程列表、网址白名单和网址黑名单等。

图表 4-83

4.1.2.5.3.13.8 敏感词审查

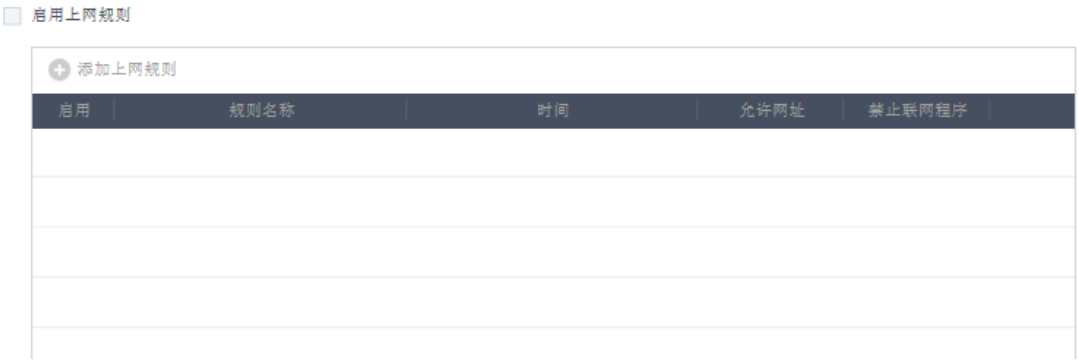
【敏感词审查】显示 v16 安全防护相关的敏感词审查策略信息，包括启用敏感词审查等。



图表 4-84

4.1.2.5.3.13.9 上网管理

【上网管理】显示 v16 安全防护相关的上网管理策略信息，包括启用上网规则等。



图表 4-85

4.1.2.5.3.13.10 其他策略

【其他策略】显示 v16 安全防护相关的其他策略信息，包括配置防火墙优先级等。

图表 4-86

4.1.2.5.3.14 杀毒（Linux）

【杀毒（Linux）】显示安全终端 Linux 杀毒相关的杀毒策略信息，包括基本设置、定时扫描策略信息。

基本设置

配置扫描优化、发现病毒时处理、清楚病毒失败时处理、隔离失败时处理、扫描路径和扫描服务器启用。

图表 4-87

定时扫描

具体操作方法请参考本文档章节 4.1.4.1 策略模板部分。

4.1.2.5.3.15 杀毒&防火墙（Linux）

【杀毒&防火墙（Linux）】显示 Linux 全功能防护客户端的杀毒&防火墙（Linux）相关策略信息，包括基本设置等策略信息。

基本设置

配置扫描优化、发现病毒时处理、文件监控和网络监控。

图表 4-88

4.1.2.5.3.16 升级与日志

【升级与日志】显示作为普通终端的虚拟机升级和日志策略信息，具体操作方法请参考本文档章节 4.1.2.4.4.2 升级与日志部分。

4.1.2.5.3.17 升级中心

【升级中心】显示作为升级服务器的虚拟机升级中心策略信息。

定时设置、网络连接设置

具体操作方法请参考本文档章节 4.1.2.4.4.2 升级与日志部分。

升级方式设置

配置升级源地址。

图表 4-89

4.1.2.5.4 日志

【日志】分为【事件日志】、【病毒查杀日志】、【隔离区】、【安全防护日志】、【网络事件日志】、【入侵防御日志】、【出站攻击日志】、【联网程序日志】和【WEB 信誉日志】。

具体操作方法请分别参考本文档章节 4.1.3.1 日志部分。

4.1.2.5.5 升级中心版本

【升级中心版本】显示升级中心版本信息，点击 立即同步 可以同步升级中心版本。

图表 4-90

4.1.3 日志报告

4.1.3.1 日志

【日志】分为【事件日志】、【病毒查杀日志】、【隔离区】、【网络事件日志】、【入侵防御日志】、【WEB 信誉日志】、【防护日志】、【出站攻击日志】、【联网程序日志】、【主动防御日志】和【木马行为防御日志】。

4.1.3.1.1 事件日志

事件日志提供了审查瑞星系统安全软件运行事件记录的功能。

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

事件日志记录信息支持条件搜索，可选条件包括：严重性以及时间范围。

图表 4-91

4.1.3.1.2 病毒查杀日志

管理中心实时收集病毒查杀结果，记录病毒查杀日志，供管理员查询以及生成各种图表、

报告使用。

病毒查杀日志信息包括查杀时间、终端、IP、中心、病毒名、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，可选条件包括病毒类型以及发现时间范围。

图表 4-92

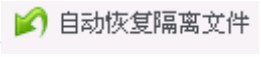
4.1.3.1.3 隔离区

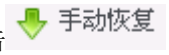
隔离的文件是已查明为（或包含）病毒且因此已进行加密并移动到安全虚拟设备中的文件。

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 4-93

勾选隔离区文件信息，点击 

，可以将隔离文件自动恢复到终端上（终端需要安装 RSTools 功能）。对于没有安装 RSTools 功能的终端，如果要恢复隔离文件，需要先勾选相应隔离文件，然后点击 

，生成相应终端的隔离文件压缩包，再点击 

，获取隔离恢复工具，然后将隔离文件压缩包和隔离恢复工具放置到相应终端上进行手动恢复。

4.1.3.1.4 网络事件日志

网络事件日志提供了 IP 规则和端口规则相关事件记录的功能。包括触发用户自定义或管理员下发的已经启用的 IP 规则、IP 黑名单、已经启用的端口禁止规则等。

网络事件日志信息包括时间、终端、IP、中心、原因、次数、动作、方向、协议、源 IP、源端口、源 MAC、目标 IP、目标端口和目标 MAC。

图表 4-94

4.1.3.1.5 入侵防御日志

入侵防御日志提供了 IDS/IPS 以及 Vpatch 相关事件记录的功能。包括黑客通过蠕虫传播、僵尸网络、木马后门、浏览器攻击、SQL 注入、远程溢出等管理员下发的已经启用的专家规则库中的方式对本系统发起的网络攻击。

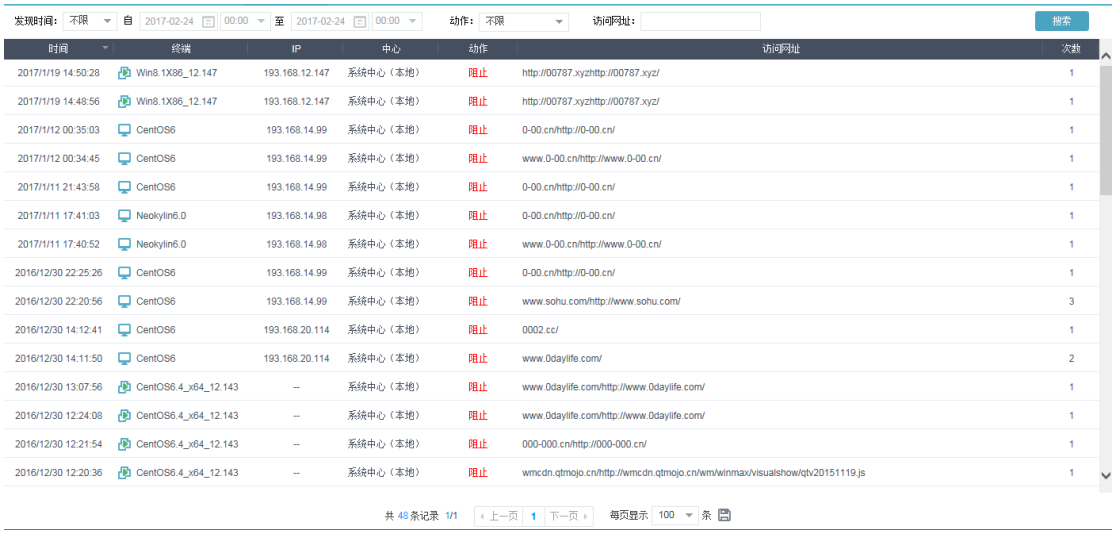
入侵防御日志信息包括时间、终端、IP、中心、原因、次数、动作、方向、协议、源 IP、源端口、目标 IP 和目标端口。

图表 4-95

4.1.3.1.6 WEB 信誉日志

WEB 信誉日志提供了上网拦截相关事件记录的功能。包括拦截钓鱼欺诈网站、木马网站、恶意下载、跨站攻击等。

WEB 信誉日志信息包括时间、终端、IP、中心、动作、访问网址和次数。



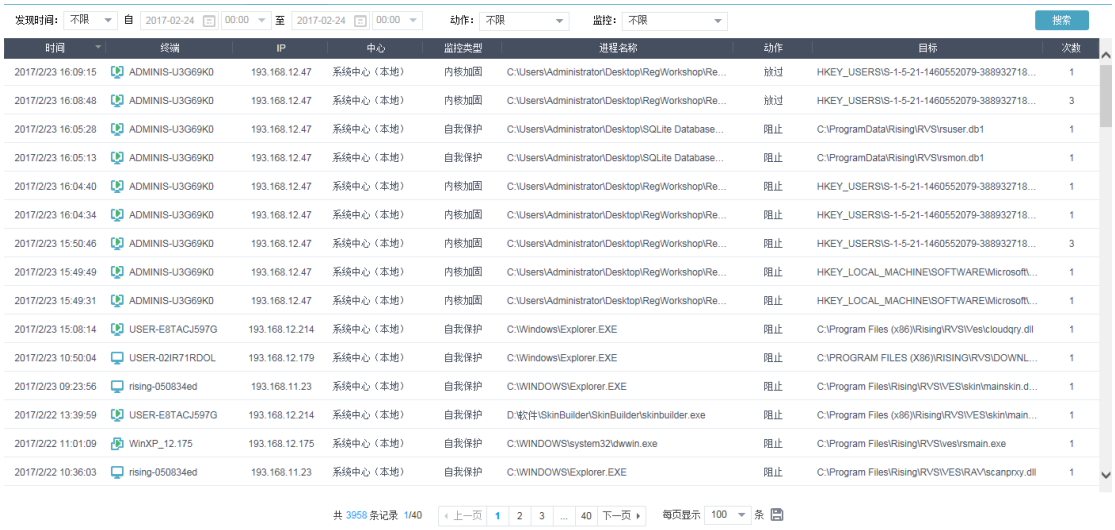
图表 4-96

4.1.3.1.7 防护日志

防护日志提供了自我保护和内核加固相关事件记录的功能。包括试图结束正在运行的瑞星杀毒软件相关进程、未经授权修改或删除系统关键文件、管理员下发的文件/注册表完整

性规则被触发等。

防护日志信息包括时间、终端、IP、中心、监控类型、进程名称、动作、目标和次数。



图表 4-97

4.1.3.1.8 出站攻击日志

出站攻击日志提供了阻止对外攻击相关事件记录的功能。包括阻止本系统因黑客入侵而对其他网络设备发起的 SYN FLOOD 攻击、ICMP FLOOD 攻击、UDP FLOOD 攻击等。

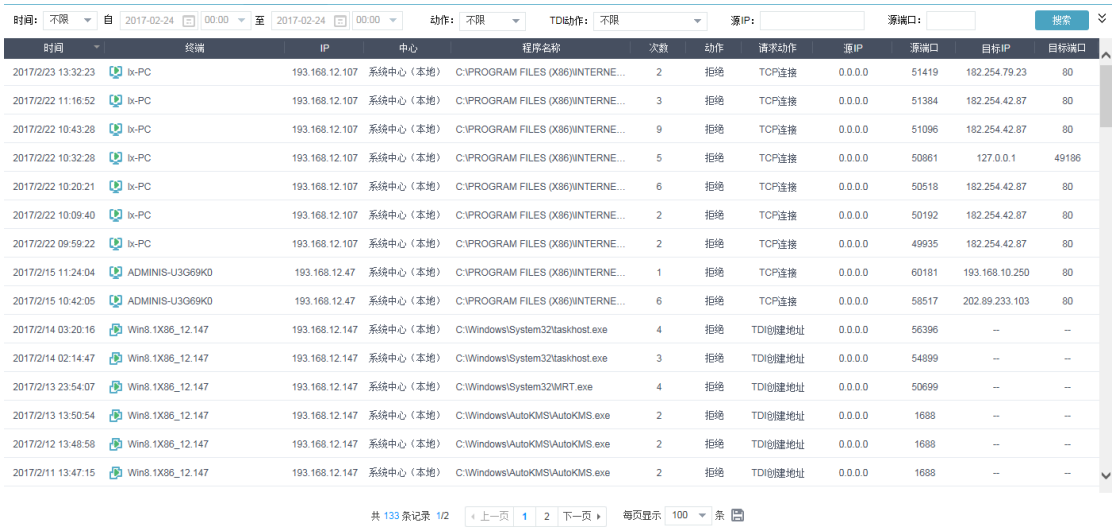
出站攻击日志信息包括时间、终端、IP、中心、攻击类型、源 IP、源端口、目标 IP、目标端口和次数。

图表 4-98

4.1.3.1.9 联网程序规则日志

联网程序规则日志提供了程序联网相关事件记录的功能。包括触发用户自定义或管理员下发的已经启用的联网程序阻止规则、按照默认拒绝联网的策略阻止未设置规则的程序连接网络、按照默认询问的策略用户主动拒绝未设置规则的程序连接网络等。

联网程序规则日志信息包括时间、终端、IP、中心、程序名称、次数、动作、请求动作、源 IP、源端口、目标 IP 和目标端口。



图表 4-99

4.1.3.1.10 主动防御日志

主动防御日志提供了自我保护相关事件记录的功能。包括试图结束正在运行的瑞星杀毒软件相关进程、未经授权修改瑞星杀毒软件相关配置、用户自定义监控的文件被访问（比如用户定义监控 c:\test.txt 不能被修改，有人试图修改该文件）、未经授权修改或删除系统关键文件、未经授权修改注册表等。

主动防御日志信息包括时间、终端、IP、中心、进程名称、来源、监控、操作、目标、次数和详情。

图表 4-100

4.1.3.1.11 木马行为防御日志

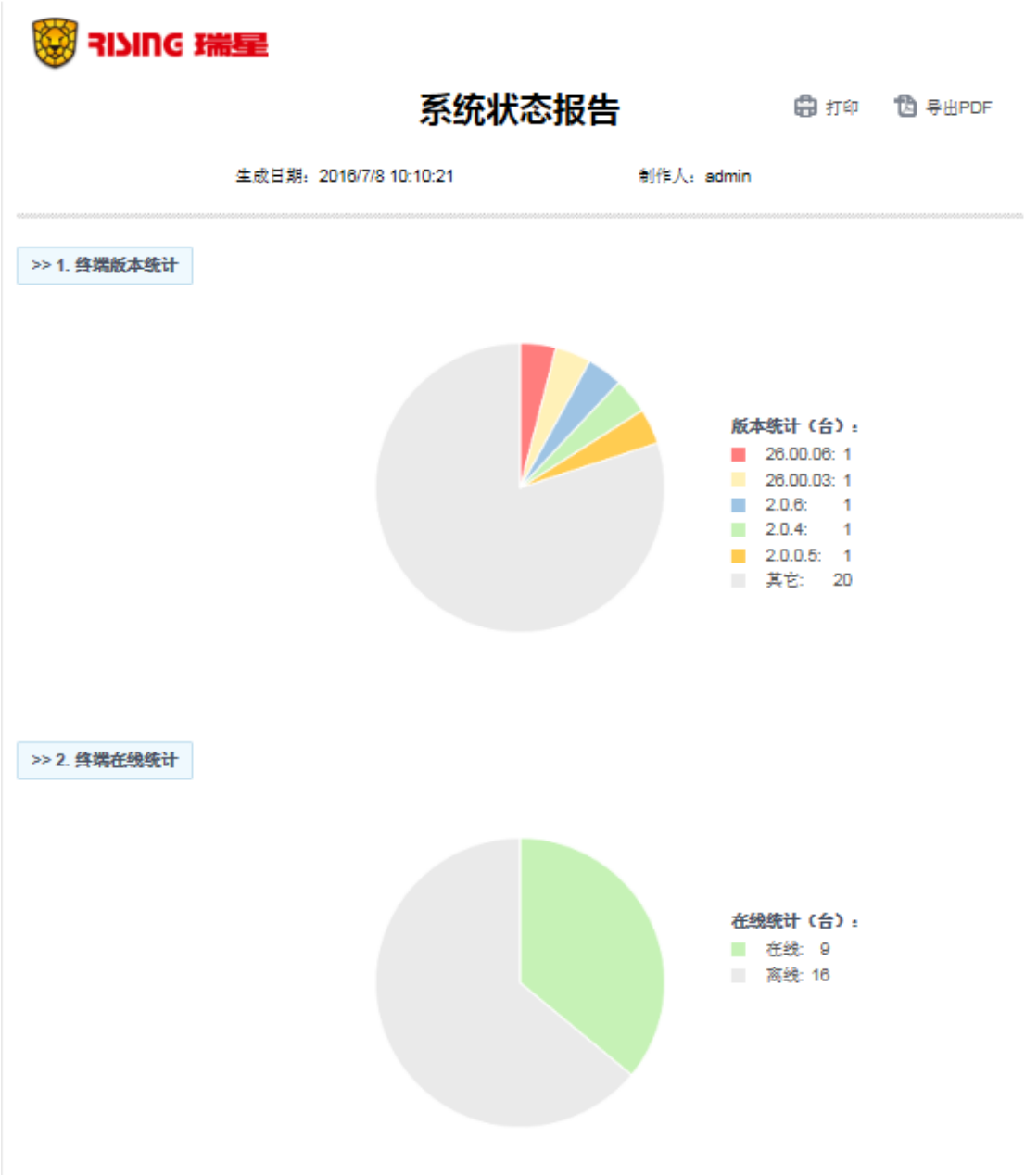
木马行为防御日志信息包括时间、终端、IP、中心、病毒名、活动进程、创建文件和次数。

4.1.3.2 报告

【报告】分为【系统状态报告】、【病毒疫情报告】、【网络安全报告】和【多维数据分析报告】。

4.1.3.2.1 系统状态报告

【系统状态报告】主要提供详尽的终端在线情况以及版本情况，支持根据筛选条件进行报告的生成、打印及导出 PDF 格式文件。



图表 4-101

4.1.3.2.2 病毒疫情报告

【病毒疫情报告】主要提供详尽的疫情趋势、终端感染情况、终端染毒排行、染毒类型、病毒排行的分析报告，支持根据筛选条件进行报告的生成、打印及导出 PDF 格式文件。

图表 4-102

4.1.3.2.3 网络安全报告

【网络安全报告】主要提供详尽的防火墙时间趋势、入侵防御时间趋势、频繁生效的防火墙规则（TOP20）、频繁生效的入侵防御规则（TOP20）、攻击源 IP（TOP20）、被攻击

IP（TOP20）、最常见的目标端口（TOP20）、访问恶意网址最多的终端（TOP20）、被访问最多的恶意网址（TOP20）的分析报告，支持根据筛选条件进行报告的生成、打印及导出 PDF 格式文件。

图表 4-103

4.1.3.2.4 多维数据分析

【多维数据分析】主要提供多维数据分析报告，可以从年份、季度、月份、查杀次数、病毒类型和来源等维度对数据进行展示与分析，支持报告的生成、打印及导出 PDF 格式文件。

图表 4-104

4.1.4 策略任务

4.1.4.1 策略模板

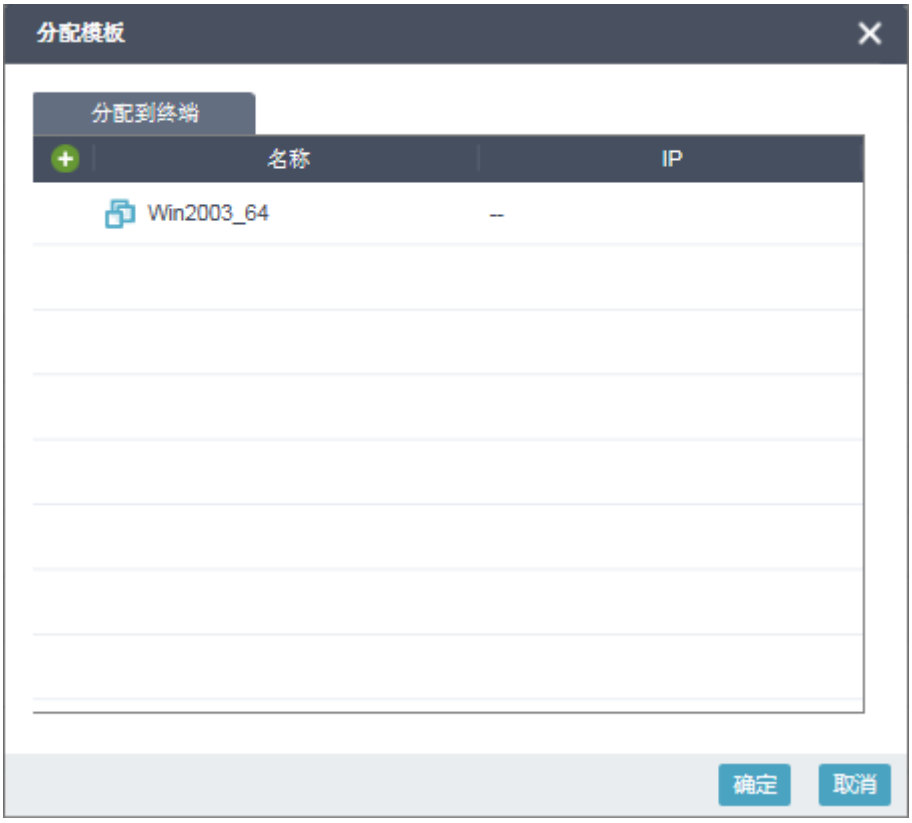
瑞星虚拟化系统安全软件支持创建各种杀毒策略和终端代理策略模板，用于下发设置至组和终端，简化管理操作。

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、类型和已分配终端数量。

策略模板信息支持条件搜索，可选条件为策略类型。

图表 4-105

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终端。



图表 4-106

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，修改策略后必须保存才有效。

图表 4-107

4.1.4.1.1 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 4-108

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 4-109

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 4-110

定义查杀目标

配置扫描的文件扩展名和目录。

图表 4-111

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 4-112

4.1.4.1.2 文件监控策略

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 4-113

监控类型设置

定义监控目标

定义排除监控目标

上述三项的具体操作方法请参考本文档章节 4.1.4.1.1 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部分。

4.1.4.2 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 4-114

点击任务事件详情查看链接，显示任务完整信息。

图表 4-115

4.1.4.3 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 4-116

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 4-117

4.1.5 系统管理

4.1.5.1 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 4-118

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 4-119

提示：角色信息请参考本文档章节4.1.5.2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。

4.1.5.2 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。

管理中心预先配置了两个角色：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 4-120

点击工具栏中的  ，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 4-121

勾选角色信息，点击工具栏中的  ，可以进行角色的删除操作。

提示：系统管理员角色无法删除。

4.1.5.3 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、有效日期、授权数量、已使用情况以及状态。

导入授权

产品	有效日期	授权数量	已使用	状态	
管理控制中心	2016/05/19 至 2019/05/20	1	1	有效	详情
VMware无代理杀毒	2016/05/19 至 2019/05/20	10	2	有效	详情
Huawei无代理杀毒	2016/05/19 至 2019/05/20	10	0	有效	详情
Linux防护(杀毒)	2016/05/19 至 2019/05/20	20	1	有效	详情
Linux防护(全功能)	2016/05/19 至 2019/05/20	20	2	有效	详情
终端防护(虚拟桌面)	2016/05/19 至 2019/05/20	100	0	有效	详情
终端防护(客户端)	2016/05/19 至 2019/05/20	50	3	有效	详情
终端防护(服务器)	2016/05/19 至 2019/05/20	50	0	有效	详情

图表 4-122

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股份有限公司联系。获得新授权证书后的导入操作方法请参考本文档章节3.3.1 导入授权证书。

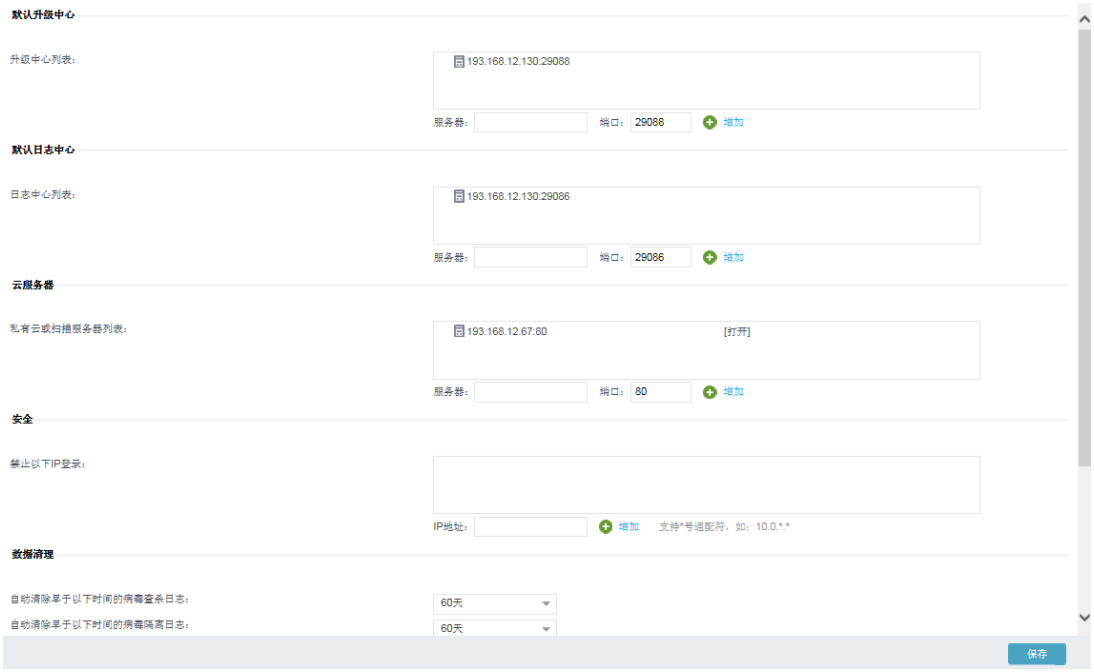
4.1.5.4 升级

升级窗口提供对产品升级包上传的管理，包括升级文件的选择和上传。

图表 4-123

4.1.5.5 设置

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、云服务器、安全和数据清理策略。

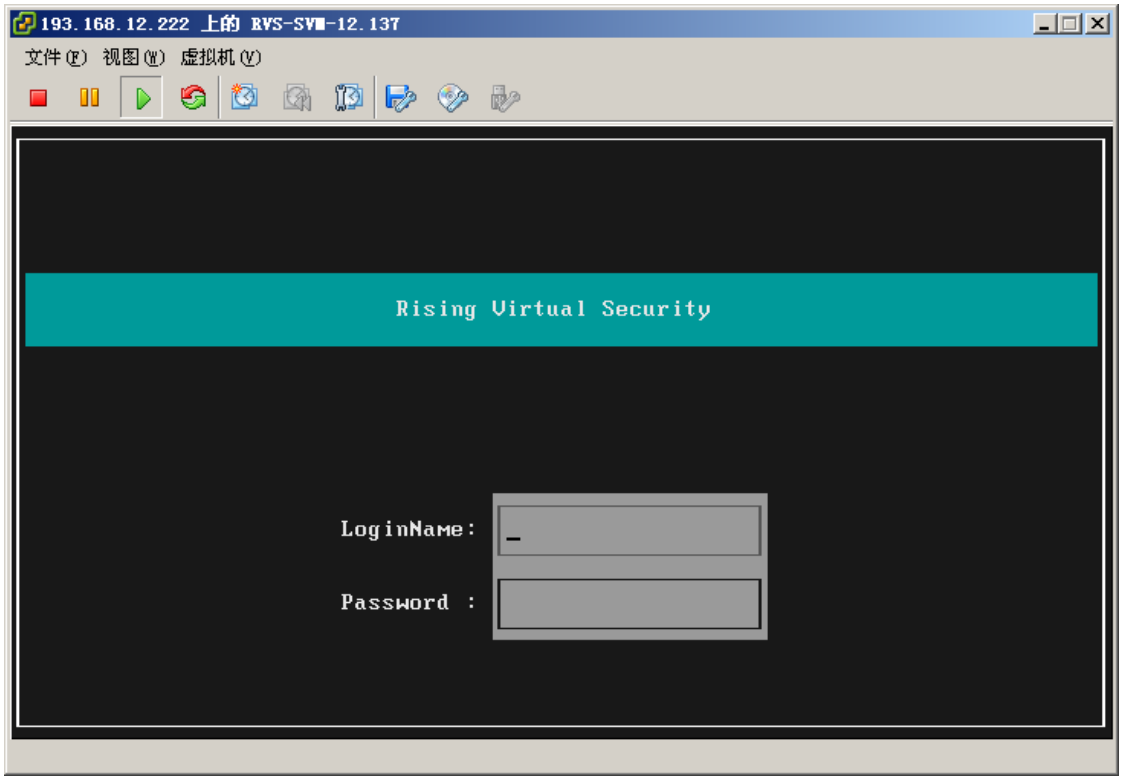


图表 4-124

4.2 VMware 无代理杀毒（vShield）

4.2.1 安全虚拟设备

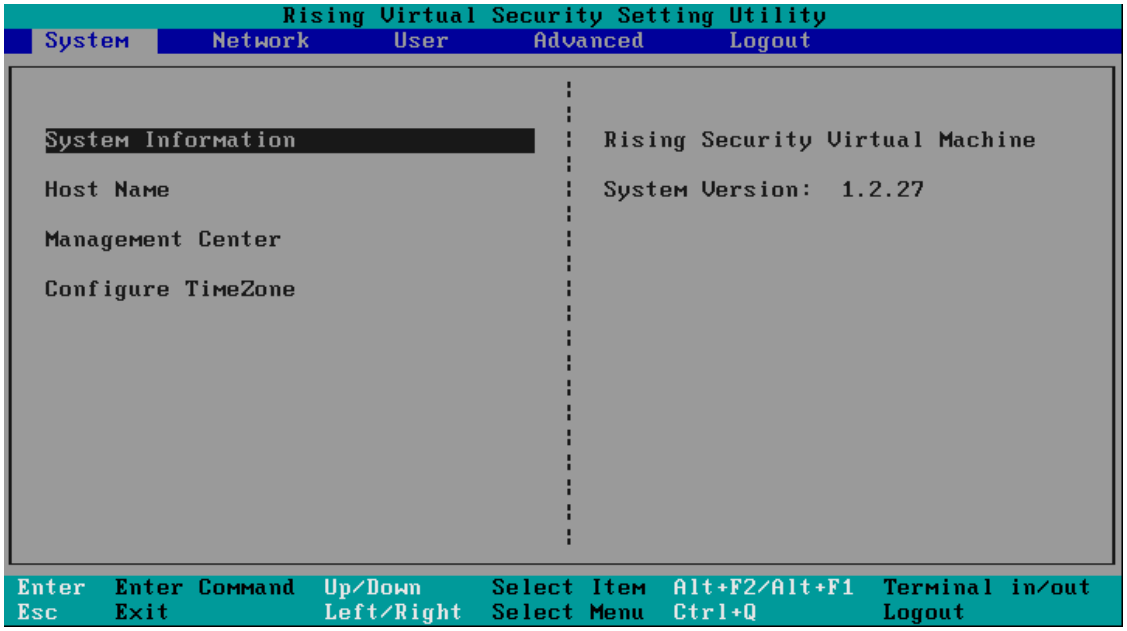
通过 vSphere Client 登录到 vCenter，找到安全虚拟设备对应的虚拟机，并启动该虚拟机控制台，显示安全虚拟设备登录界面。



图表 4-125

4.2.1.1 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。

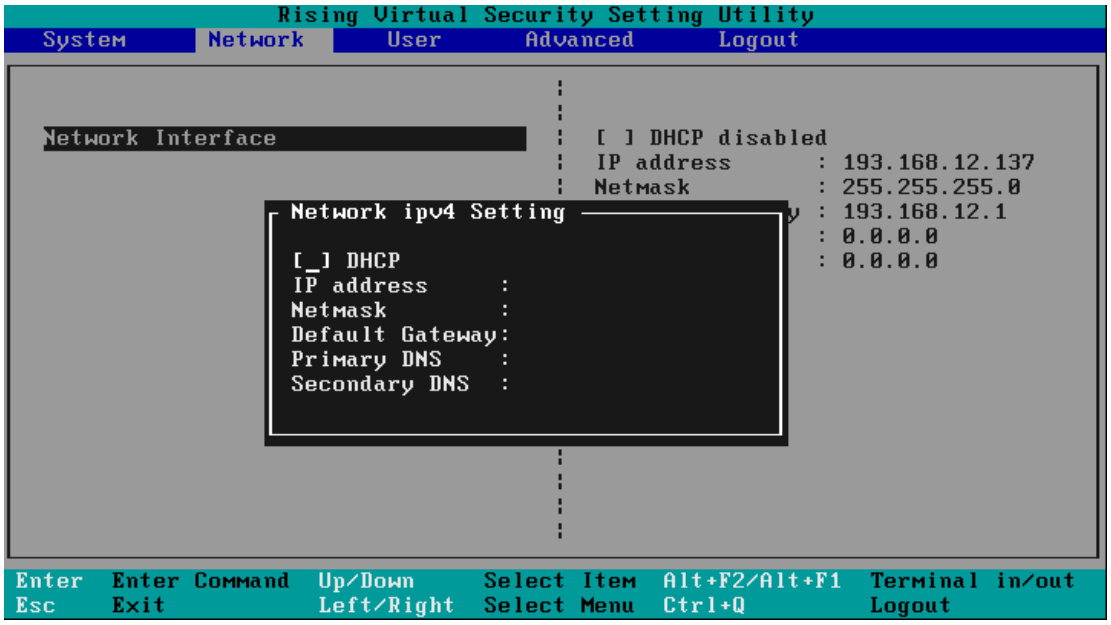


图表 4-126

4.2.1.2 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。

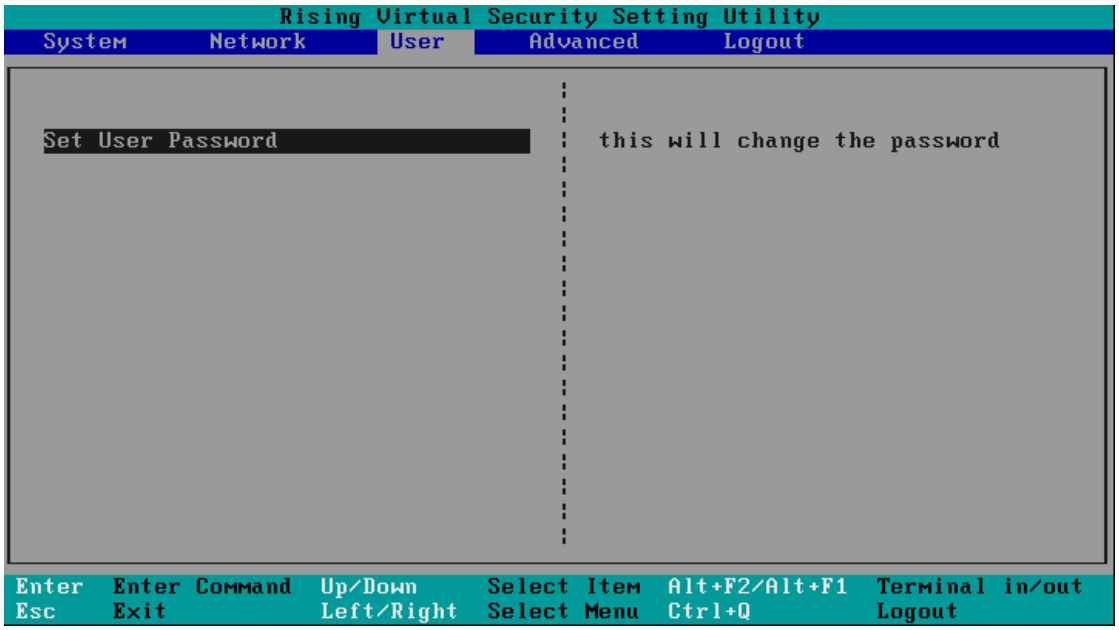
安全虚拟设备缺省使用本地 DHCP 服务器分配的 IP 地址。如果没有 DHCP 服务器，回车后手动输入 IP 地址信息。



图表 4-127

4.2.1.3 配置密码

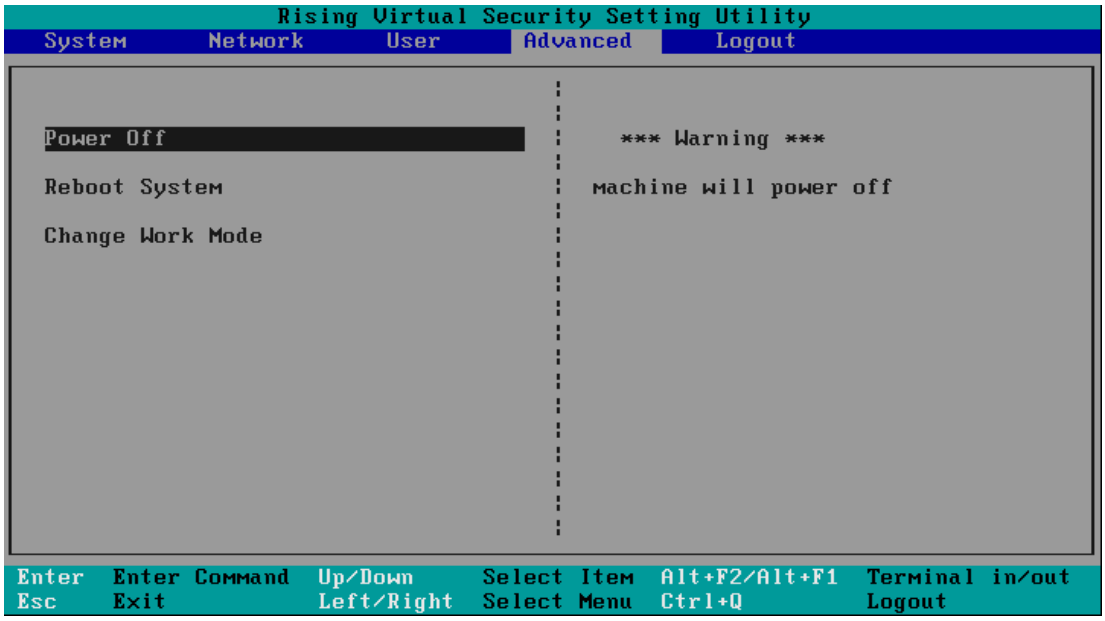
选中【USER】页签，显示【Set User Password】设置安全虚拟设备管理员密码。



图表 4-128

4.2.1.4 重启系统

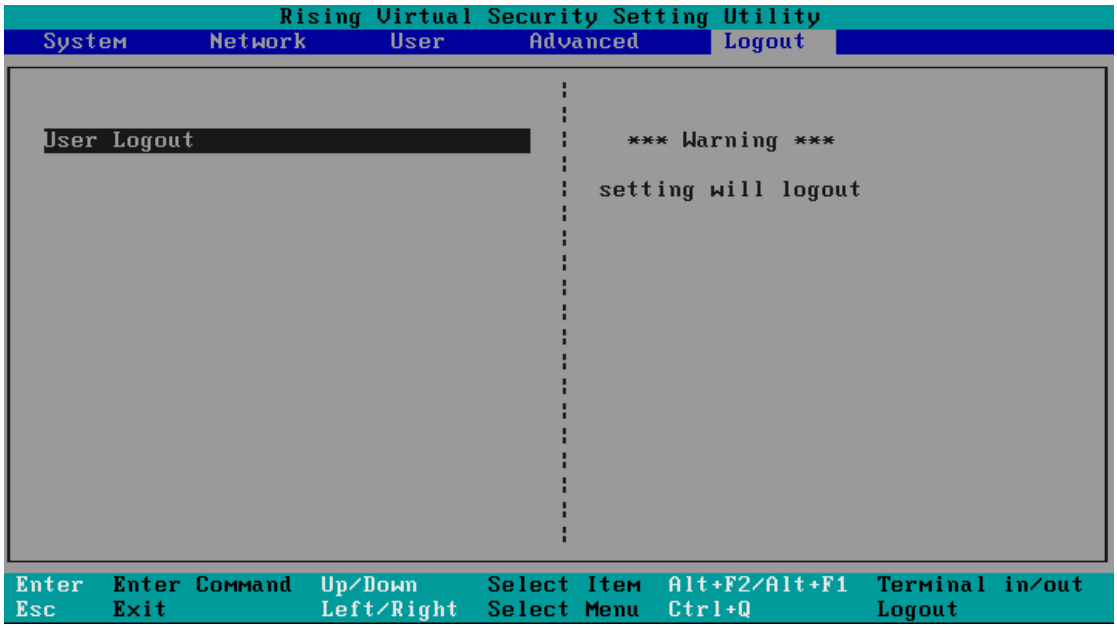
选中【Advanced】页签，显示【Power Off】执行关闭或【Reboot System】重启安全虚拟设备的操作，以及【Change Work Mode】改变工作模式。关闭或重启前，将自动保存此前的配置信息。



图表 4-129

4.2.1.5 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 4-130

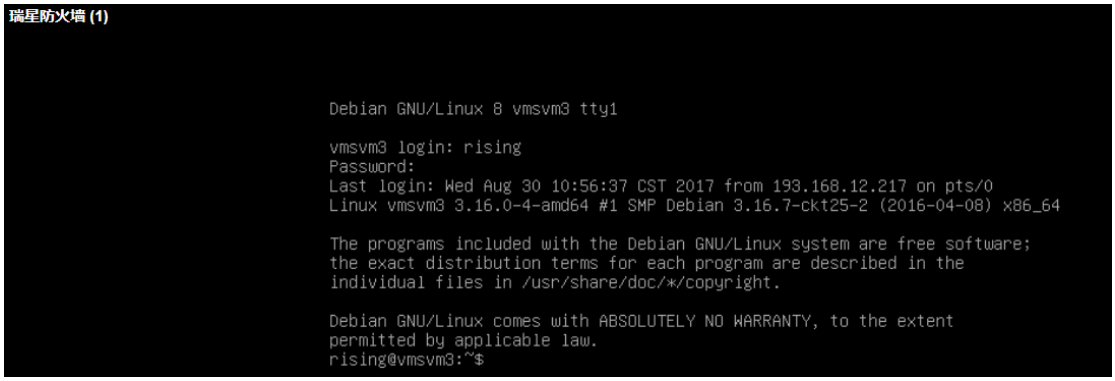
4.3 VMware 无代理杀毒（NSX）

4.3.1 安全虚拟设备

通过 vSphere Web Client 登录到 vCenter，找到安全虚拟设备对应的虚拟机。

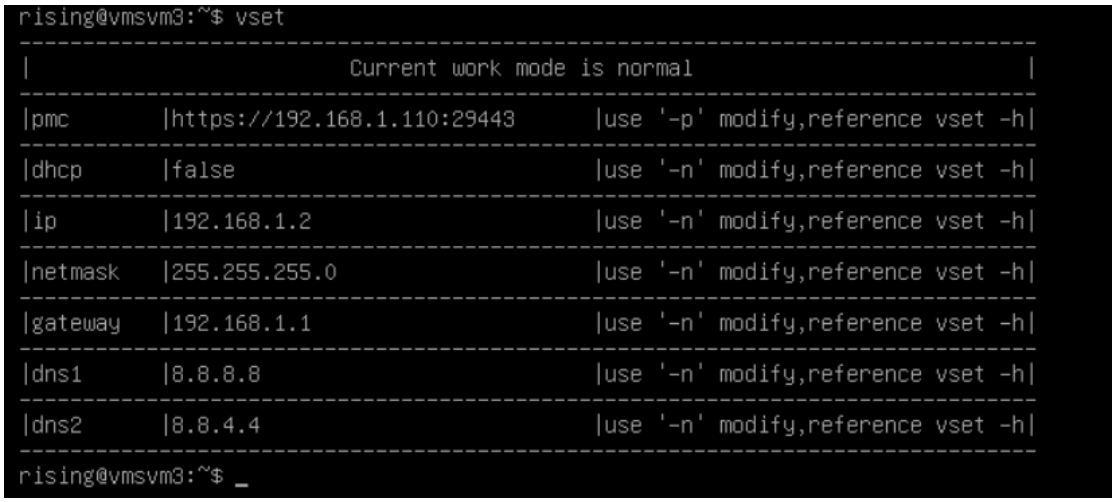
启动该虚拟机控制台，显示安全虚拟设备登录界面。

使用账户 rising 登录系统，默认密码为 rising。此帐户为低权限帐户，但仍建议登录后修改默认密码。



4.3.1.1 系统信息

输入 vset 命令可以查看当前 SVM 的配置。



图表 4-131

4.3.1.2 配置管理网络及管理中心

通常不需要用户手动配置网络或者管理中心，应当由 NSX 创建虚拟机时分配指定。当用户确实需要重新修改网络 IP 时，可以通过 vset 命令修改。详细参考 vset -h 帮助说明。

```
usage vset [-h]|[-l]|[-m debug|normal]|[-n network config]|[-p PMC CONFIG]
    -h:print this help message.
    -l:To view the SVM configuration information.
    -m:Set the SVM operating mode.
        1.Set the work mode to DEBUG: vset -m debug
        2.Set the work mode to NORMAL: vset -m normal
    -n:Set the SVM network information.
        1.Set to obtain IP address automatically: vset -n dhcp=true
        2.Set the IP address: vset -n ip=xxx.xxx.xxx.xxx netmask=xxx.xxx.xxx.xxx
        3.Set the gateway: vset -n gateway=xxx.xxx.xxx.xxx
        4.Set the DNS: vset -n dns=xxx.xxx.xxx.xxx (Set up multiple DNS address with ',' separated )
    -p:Set pmc configuration information.
        1.Using IP address design: vset -p 192.168.1.1
        2.Using domain name design: vset -p https://www.xxxx.com
```

通过帮助说明可知，可以使用-p 参数配置管理中心地址，使用-n 参数可以配置管理网络 IP 等。

配置网络 IP 示例：

vset -n ip=193.168.1.123 netmask=255.255.255.0 gateway=193.168.1.1

配置管理中心示例：

vset -p 193.168.12.110

或

vset -p https://domainName.com

当配置管理中心时使用了域名解析的方式，则需要配置 DNS，示例：

vset -n dns=8.8.8.8,8.8.4.4

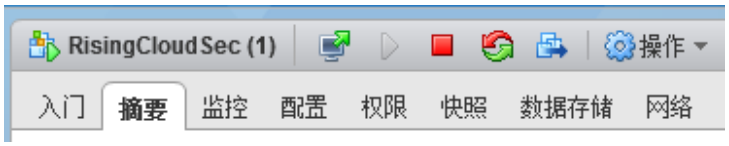
4.3.1.3 配置密码

修改 rising 用户的密码，修改方法即 linux 系统下用户密码修改密码，使用 passwd 命令。

```
rising@vmsvm3:~$ passwd
Changing password for rising.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
```

4.3.1.4 重启系统

可通过 vSphere Web Client 虚拟机页面，选择关机或者重启。



4.3.1.5 退出系统

执行 exit 命令，退出安全虚拟设备登录界面。

4.4 HUAWEI 无代理杀毒

4.4.1 安全虚拟设备

具体操作方法请参考本文档章节 4.2.1 安全虚拟设备。

4.5 安全防护终端

安全防护终端分为常用设置和扩展设置。常用设置是管理中心和安全防护终端都可以进行的设置。扩展设置是安全防护终端独有的设置，只能通过客户端设置。如需设置扩展功能，需要联系管理中心管理员获得客户端设置修改权限。

4.5.1 常用设置

常用设置包括病毒查杀、智能主动防御、实时监控、网络攻击防护和访问控制。

4.5.1.1 病毒查杀

4.5.1.1.1 手动查杀

详情请参考本文档章节 4.1.2.5.4.7 杀毒（Windows）手动扫描。

4.5.1.1.2 空闲时段查杀

详情请参考本文档章节 4.1.2.5.4.7 杀毒（Windows）定时扫描。

4.5.1.2 智能主动防御

智能主动防御设置包括系统加固、应用程序控制、木马行为防御、木马入侵拦截（U 盘拦截）、木马入侵拦截（网站拦截）和瑞星自我保护功能等。

4.5.1.2.1 系统加固设置

详情请参考本文档章节 4.1.2.5.4.9 主动防御（Windows）系统加固。

4.5.1.2.2 应用程序控制设置

详情请参考本文档章节 4.1.2.5.4.9 主动防御（Windows）应用程序控制。

4.5.1.2.3 木马行为防御设置

详情请参考本文档章节 4.1.2.5.4.9 主动防御（Windows）木马行为防御。

4.5.1.2.4 木马入侵拦截（U 盘拦截）设置

详情请参考本文档章节 4.1.2.5.4.9 主动防御（Windows）U 盘拦截

4.5.1.2.5 木马入侵拦截（网站拦截）设置

详情请参考本文档章节 4.1.2.5.4.9 主动防御（Windows）网站拦截。

4.5.1.2.6 自我保护设置

详情请参考本文档章节 4.1.2.5.4.9 主动防御（Windows）自我保护。

4.5.1.3 实时监控

详情请参考本文档章节 4.1.2.5.4.7 杀毒（Windows）文件监控。

4.5.1.4 网络攻击防护

4.5.1.4.1 恶意网址拦截

详情请参考本文档章节 4.1.2.5.4.8 防火墙（Windows）恶意网址。

4.5.1.4.2 网络攻击拦截

详情请参考本文档章节 4.1.2.5.4.8 防火墙（Windows）网络攻击拦截。

4.5.1.4.3 出站攻击拦截

详情请参考本文档章节 4.1.2.5.4.8 防火墙（Windows）出站攻击防御。

4.5.1.5 访问控制

详情请参考本文档章节 4.1.2.5.4.8 防火墙（Windows）IP 包过滤和 4.1.2.5.4.8 防火墙（Windows）应用程序网络访问监控。

4.5.2 扩展设置

非常用设置即扩展设置，包括开机查杀、office/IE、outlook 和其他嵌入式查杀的设置。

4.5.2.1 开机查杀

在开机查杀设置页面可以选择查杀对象，分别为所有硬盘、系统盘、Windows 系统目录以及所有的服务和驱动。

4.5.2.2 Office/IE

如果安装了 Office/IE，瑞星虚拟化系统安全软件安全防护终端能够支持对 Office/IE 的监控。

每次当您打开 Office 文档时或者用 IE 下载插件程序文件时， Office/IE 嵌入式杀毒可以自动扫描病毒，保护您系统的安全。瑞星 Office/IE 嵌入式杀毒只有在您使用 Office 2000 及以上版本或者 IE 5 及以上版本时才起作用。

启用 Office/IE 嵌入式杀毒功能

在瑞星虚拟化系统安全软件安全防护终端主程序界面中，选择【设置】/【详细设置】，选中【查杀设置】，在【使用 Office/IE 嵌入式杀毒】选项前勾选，并单击【应用】/【确定】保存设置。

图表 4-132

用户可以选择查杀级别，拖动滑块选择高、中、低三种级别，也可以自定义查杀级别。


设置
查杀设置
手动查杀
空闲时段查杀
Office/IE
Outlook
其它嵌入式杀毒
监控设置
网络监控
其它设置
中安全级别
推荐的最佳级别
适用大部分用户
引擎配置的最佳平衡点
自定义级别
恢复默认级别
处理方式
查杀文件类型
发现病毒时：
清除病毒
杀毒失败时：
不处理
隔离失败时：
不处理
确定(O)
取消(C)
应用(A)
帮助(H)

图表 4-133

图表 4-134

查杀文件类型：

- 所有文件
- 仅查杀可执行文件（如：EXE、COM、DLL 等）
- 自定义扩展名（多个扩展名需用英文状态的分号隔开）

勾选【隐藏杀毒结果】后，瑞星虚拟化系统安全软件安全防护终端主程序查杀病毒时，不显示杀毒结果。

4.5.2.3 Outlook

如果安装了 Outlook，瑞星虚拟化系统安全软件安全防护终端能够支持对 Outlook 的监控。

每次当您打开 Outlook 文档时文件时， Outlook 嵌入式杀毒可以自动扫描病毒，保护您系统的安全。

启用 Outlook 嵌入式杀毒功能

在瑞星虚拟化系统安全软件安全防护终端主程序界面中，选择【设置】/【详细设置】，选中【查杀设置】，在【使用 Outlook 嵌入式杀毒】选项前勾选，并单击【应用】/【确定】保存设置。

图表 4-135

用户可以选择查杀级别，拖动滑块选择高、中、低三种级别，也可以自定义查杀级别。


设置
查杀设置
手动查杀
空闲时段查杀
Office/IE
Outlook
其它嵌入式杀毒
监控设置
网络监控
其它设置
中安全级别
推荐的最佳级别
适用大部分用户
引擎配置的最佳平衡点
自定义级别
恢复默认级别
处理方式
查杀文件类型
查杀方式
发现病毒时：
清除病毒
杀毒失败时：
不处理
隔离失败时：
不处理
确定(O)
取消(C)
应用(A)
帮助(H)

图表 4-136

图表 4-137

查杀文件类型：

- 所有文件
- 仅查杀可执行文件（如：EXE、COM、DLL 等）
- 自定义扩展名（多个扩展名需用英文状态的分号隔开）

勾选【隐藏杀毒结果】后，瑞星虚拟化系统安全软件安全防护终端主程序查杀病毒时，不显示杀毒结果。

图表 4-138

查杀方式：

- 发送邮件时查杀病毒
- 接受邮件时查杀病毒
- 打开邮件时查杀病毒

扫描方式可根据实际需求勾选部分或者全部勾选。

4.5.2.4 其他嵌入式杀毒

其他嵌入式杀毒指除了以上方式外，用户可以自定义的查杀设置。

启用其他嵌入式杀毒功能

在瑞星虚拟化系统安全软件安全防护终端主程序界面中，选择【设置】/【详细设置】，选中【查杀设置】。

图表 4-139

点击右下角的 设定其它嵌入式杀毒 按钮，进入其他嵌入式杀毒设置界面。

图表 4-140

若已经有提示可能被病毒利用的软件显示在展示栏中，点击软件图标，点击【开启】，开启对该软件的嵌入式查杀。

图表 4-141

- 勾选【当嵌入式杀毒设置工具升级时，自动嵌入所有支持的软件。】，软件将为用户自动添加支持所有支持的软件。

- 勾选【显示所有支持的软件】，显示全部支持软件。

图表 4-142

用户可以选择查杀级别，拖动滑块选择高、中、低三种级别，也可以自定义查杀级别。

图表 4-143

4.6 全功能安全防护客户端

全功能安全防护客户端的设置包括客户端本地查杀设置和管理中心远程扫描设置两部分，分别对应客户端本地操作和管理中心远程扫描指令。

4.6.1 客户端本地查杀设置

4.6.1.1 病毒查杀设置

单击【病毒查杀】页面的 查杀设置，进行病毒查杀设置。包括病毒处理设置、文件类型、病毒处理、扫描计划。

图表 4-144

4.6.1.2 网络防护设置

网络防护包括 IDS/IPS、Vpatch、WEB 信誉、阻止攻击和敏感词审查。

图表 4-145

4.6.1.2.1 联网程序规则

单击 联网程序规则，进入联网程序规则页面，可以增加、编辑、删除、导入和导出联网程序规则。

图表 4-146

4.6.1.2.2 IP 上网规则

单击 IP上网规则，进入 IP 上网规则页面，可以增加、编辑、删除、导入和导出 IP 上网规则。

图表 4-147

4.6.1.2.3 端口规则

单击 端口规则，进入端口规则页面，可以增加、编辑、删除、导入和导出端口规则。

图表 4-148

4.6.1.3 软件设置

“软件设置”是用户详细设置全功能安全防护客户端的各功能界面，用户可在全功能安全防护客户端右上角点击“菜单”按钮。

图表 4-149

然后点击“软件设置”。

图表 4-150

之后就会打开“软件设置”的主界面，其中包括 “常规设置”、“云安全”、“查杀白名单”、“升级计划”、 “升级网络”和“其他设置”。

4.6.1.3.1 常规设置

常规设置包括“开机启动”、“自我保护”和“免打扰”等设置。

图表 4-151

4.6.1.3.2 云安全

云安全包括启用瑞星云安全系统、设置私有云和公有云连接。

图表 4-152

4.6.1.3.3 查杀白名单

查杀白名单包括添加、导入、导出和批量删除查杀白名单。

图表 4-153

4.6.1.3.4 升级计划

升级计划包括“升级模式设置”和“升级计划”等设置。

图表 4-154

点击“修改周期”，可以修改升级的日期和开始时间。

图表 4-155

4.6.1.3.5 升级网络

升级网络包括“代理类型”和“代理服务器设置”等设置。

图表 4-156

4.6.1.3.6 其他设置

其他设置包括“日志设置”和“病毒隔离区”等设置。

图表 4-157

4.6.2 管理中心远程扫描设置

详细请参考本文档章节 4.1.2.5.4.11 杀毒。

4.7 安全终端 Linux 杀毒

安全终端 Linux 杀毒的设置包括客户端本地查杀设置和管理中心远程扫描设置两部分，分别对应客户端本地查杀操作和管理中心远程扫描指令。

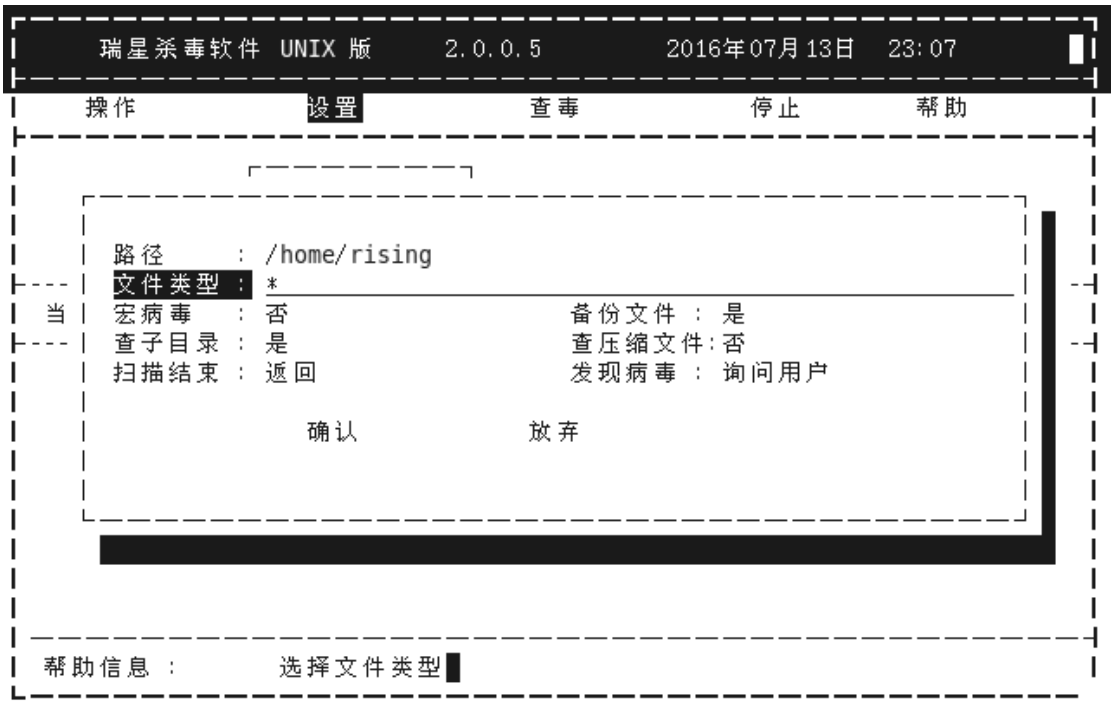
4.7.1 客户端本地查杀设置

4.7.1.1 字符界面设置

第一次启动程序的功能设置是默认的，可以在菜单栏的【设置】菜单中按需要设置软件所有的选项。

图表 4-158

4.7.1.1.1 查杀设置



图表 4-159

【路径】：用于设置查杀目录，第一次启动时是默认路径，用户可以进行修改并通过“操作”菜单保存修改后的设置。

【文件类型】：用于选择查杀文件的类型。

【宏病毒】：用于对宏病毒处理方法的选择。

【备份文件】：用于设置备份隔离病毒文件。

【查子目录】：选择是否查子目录。

【查压缩文件】：选择是否查压缩文件。

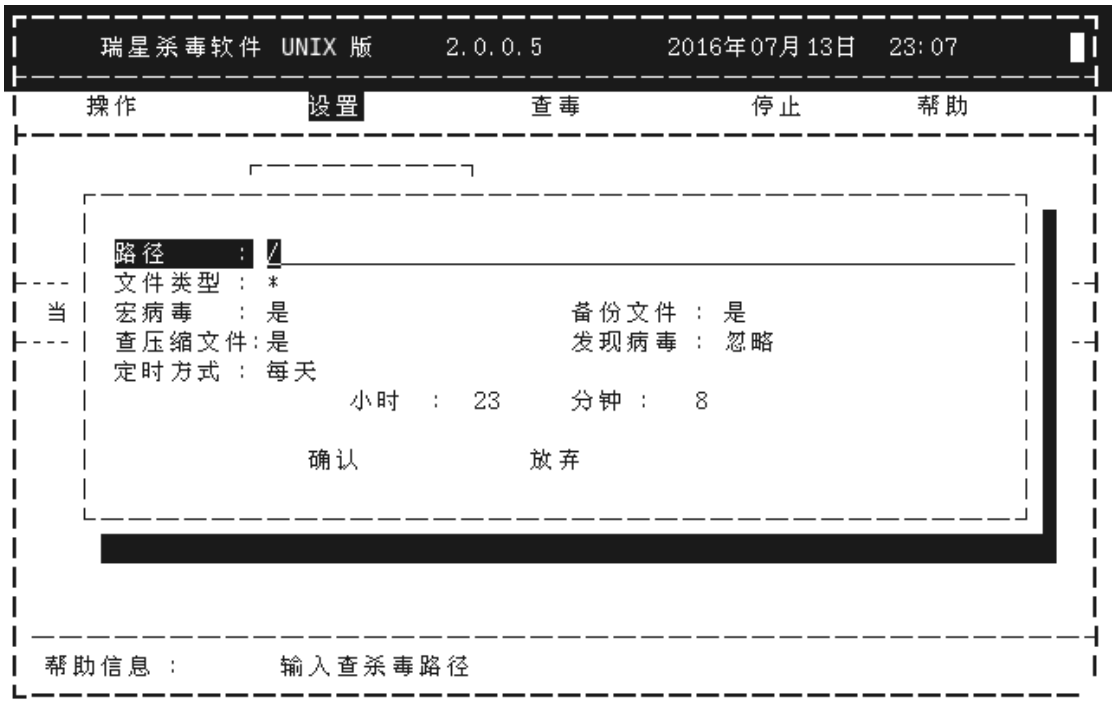
【扫描结束】：选择返回主界面或退出程序。

【发现病毒】：选择发现病毒后的处理方式。如果选择了【询问用户】，则在发现病毒后会弹出询问窗口。程序会向用户询问如何处理，处理方式有【清除病毒】、【删除被感染文件】、【忽略该病毒，继续】和【停止】。如果想一直使用某种处理方式，请使用空格键或回车键选中【总是使用该选项】（若选择【停止】则无需选中【总是使用该选项】）。

图表 4-160

4.7.1.1.2 定时设置

最下面一项用来设置定时查杀的频率和具体时间。

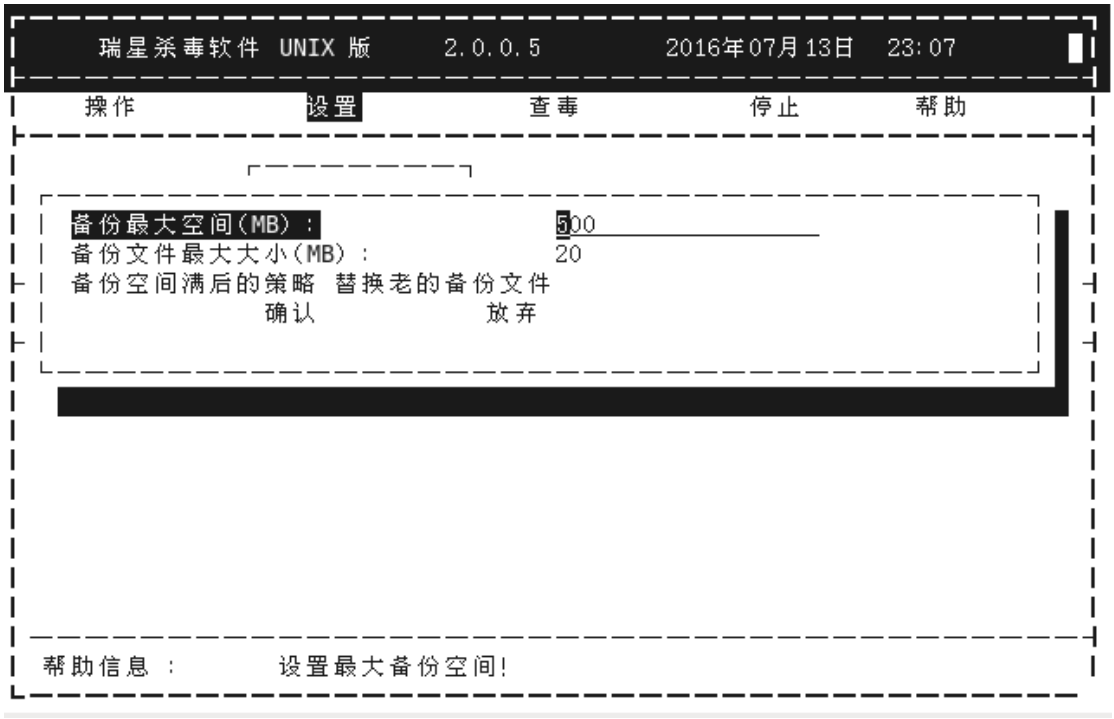


图表 4-161

4.7.1.1.3 隔离设置

主要用于隔离病毒文件的位置及大小的设置。

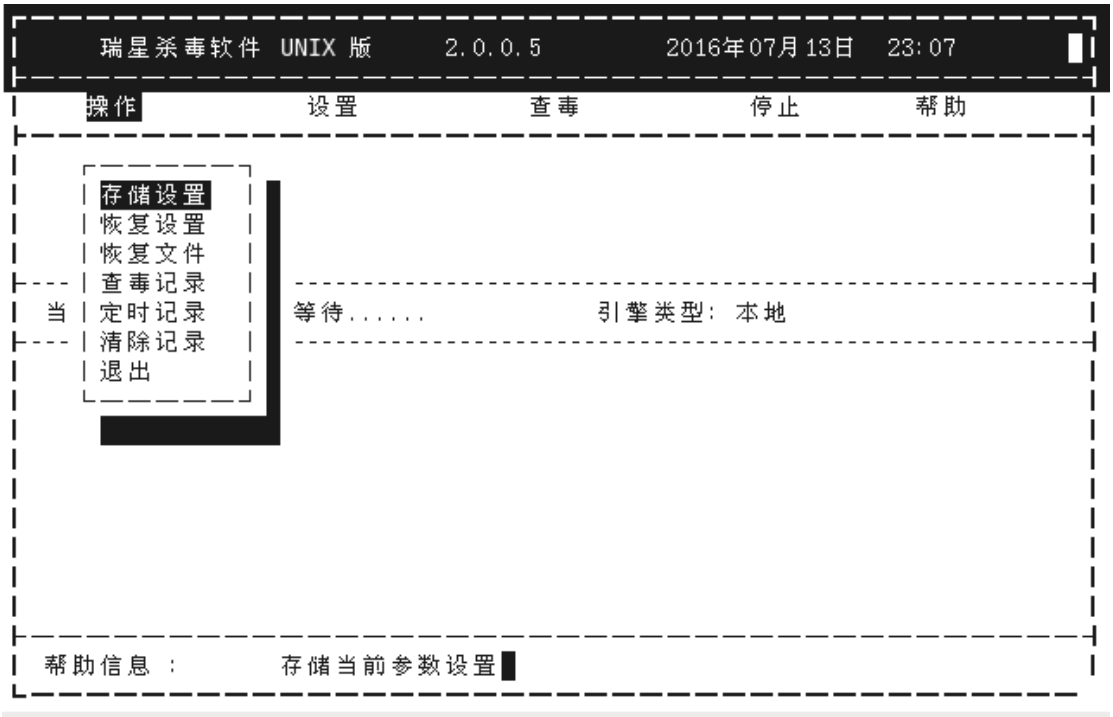
提示：用户只要执行查杀后“隔离设置”中的参数会自动保存。



图表 4-162

4.7.1.1.4 其他设置

其他设置包含存储设置、恢复设置、恢复文件、查毒记录、定时记录、清除记录和退出。



图表 4-163

【存储设置】：用于保存设置参数。

提示：如果不保存查杀路径，每一次查杀均需要设置查杀路径。

【恢复设置】：恢复最近一次存储的参数设置。

【恢复文件】：用于对以往杀毒时隔离的病毒文件作恢复处理，可以将光标移到要恢复或者清除的文件列表上面，用回车或者空格键选中，也可以使用【全选】，再使用 Tab 键或方向键选择【恢复】、【删除】或者【取消】，完成对隔离病毒文件的处理。

图表 4-164

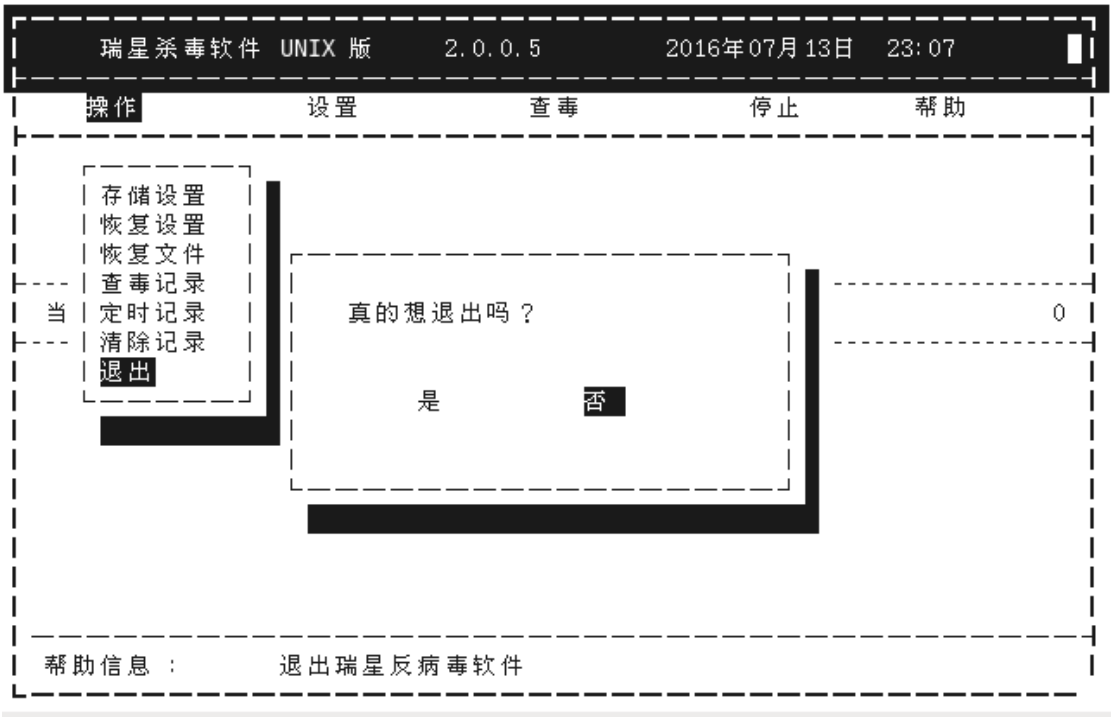
【查毒记录】：查看以前的查毒历史记录。

图表 4-165

【定时记录】：查看以前的定时查杀记录。

【清除记录】：用于清除以上所述的各项历史记录。

【退出】：退出程序，选择并执行该项，程序会询问是否真正退出，可根据选项进行选择，选择【是】则退出；选择【否】则返回主界面。



图表 4-166

4.7.1.2 图形界面设置

图表 4-167

【手动扫描设置】：对查杀参数进行详细的设置。

【定时扫描】：对定时查杀参数进行设置。

【网络设置】：用户可以根据自己的网络连接方式，设置上网升级的网络配置。

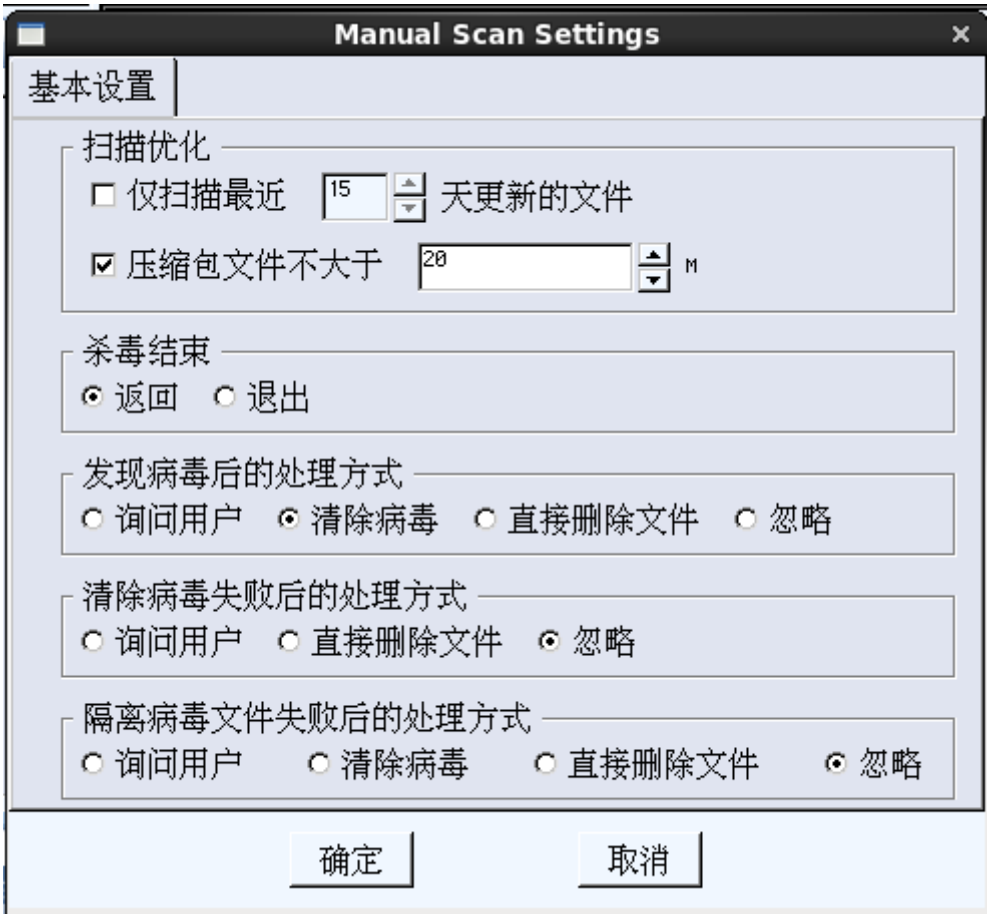
【私有云设置】：可以设置本地库或者使用云引擎，设置私有云地址。

【管理中心设置】：用于用户设置和修改管理中心的地址端口号。

【其它设置】：对系统的一些其它参数进行设置。

4.7.1.2.1 手动扫描设置

在程序的主界面，选择菜单【设置】/【手动扫描设置】，打开手动扫描设置界面。



图表 4-168

【优化扫描】：可以选择扫描最近几天更新的文件（勾选并设置需要扫描的天数）、压缩包文件不大于某个值（具体参数自行设置，默认为 20M）。

【杀毒结束时】：杀毒结束后有返回和退出两种操作；

【发现病毒时】：发现病毒时有询问用户、清除病毒、直接删除文件、忽略四种处理方式；

【清除病毒失败时】：可采取询问用户、直接删除文件和忽略三种处理方式；

【隔离病毒文件失败后的处理方式】：病毒隔离失败时，可选择是否询问用户，也可选择清除病毒、直接删除文件、忽略三种中的一种处理方式。

4.7.1.2.2 定时扫描

定时扫描功能是在指定时刻，瑞星杀毒软件自动在后台运行，对预先设置的目录进行扫描。此功能使用户即使在无人值守的情况下，查杀病毒保证计算机的安全。

在程序的主界面，选择菜单【设置】/【定时扫描】，打开定时扫描设置界面。

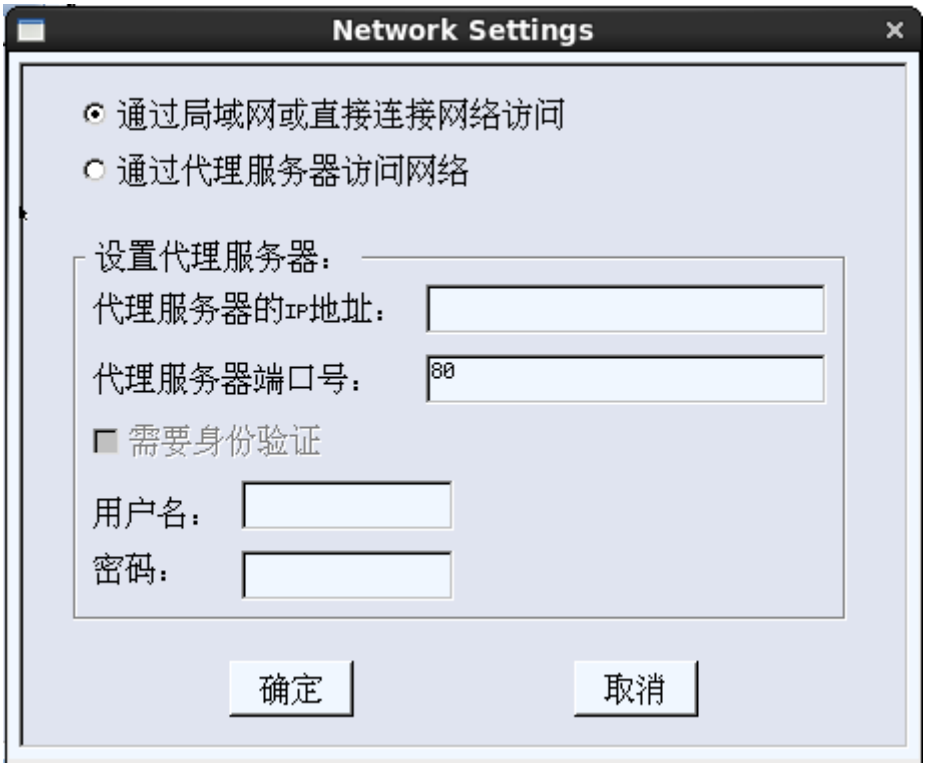
图表 4-169

【扫描路径】：点击浏览按钮，选择需要进行定时扫描的文件路径；

【定时扫描设置】：为定时扫描设定具体的查杀频率和时间。需要选择扫描频率后才能设置扫描时刻。

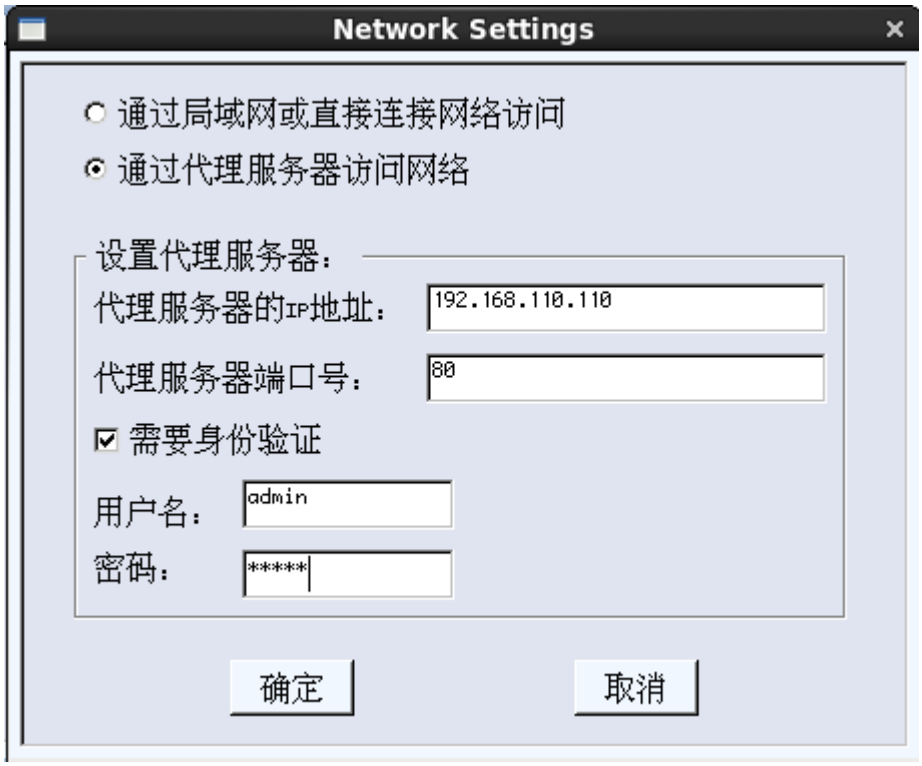
4.7.1.2.3 网络设置

在程序的主界面，选择菜单【设置】/【网络设置】，打开网络设置界面。



图表 4-170

默认选择的网络连接方式为“通过局域网或直接连接网络访问”，您也可以选择“通过代理服务器访问网络”。勾选“通过代理服务器访问网络”后，“需要身份验证”区域由灰色变为可编辑状态，将“代理服务器的 IP 地址”、“代理服务器的端口号”填写好；如果需要身份验证，请勾选身份验证，并填写“用户名”、“用户密码”，点击确定完成设置。

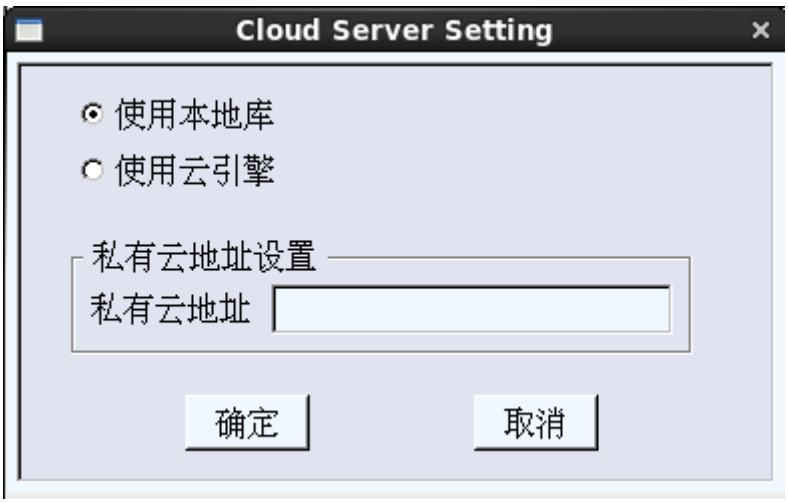


图表 4-171

4.7.1.2.4 私有云设置

在程序的主界面，选择菜单【设置】/【私有云设置】，打开私有云设置界面。

私有云设置可以选择查杀引擎，设置私有云地址。



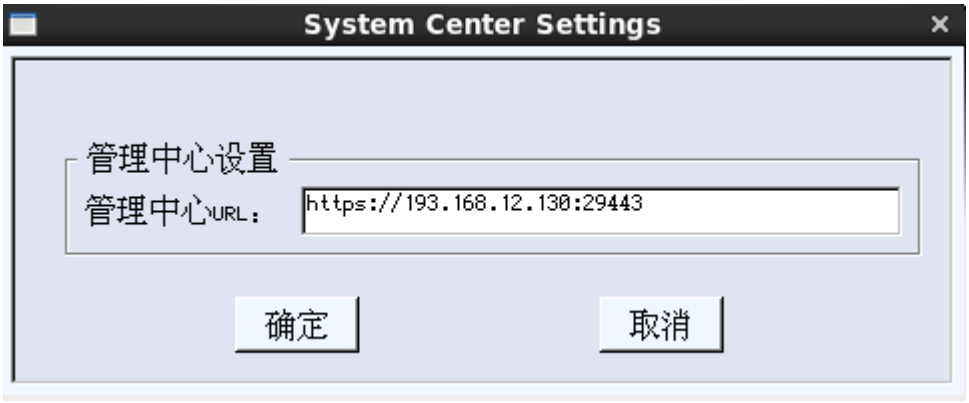
图表 4-172

选择使用本地库，扫描时默认启用本地引擎进行查杀；

选择使用云引擎，扫描时默认启用云引擎进行查杀，并且在私有云地址栏输入私有云的地址和端口。

4.7.1.2.5 管理中心设置

在程序的主界面，选择菜单【设置】/【管理中心设置】，打开管理中心设置界面。



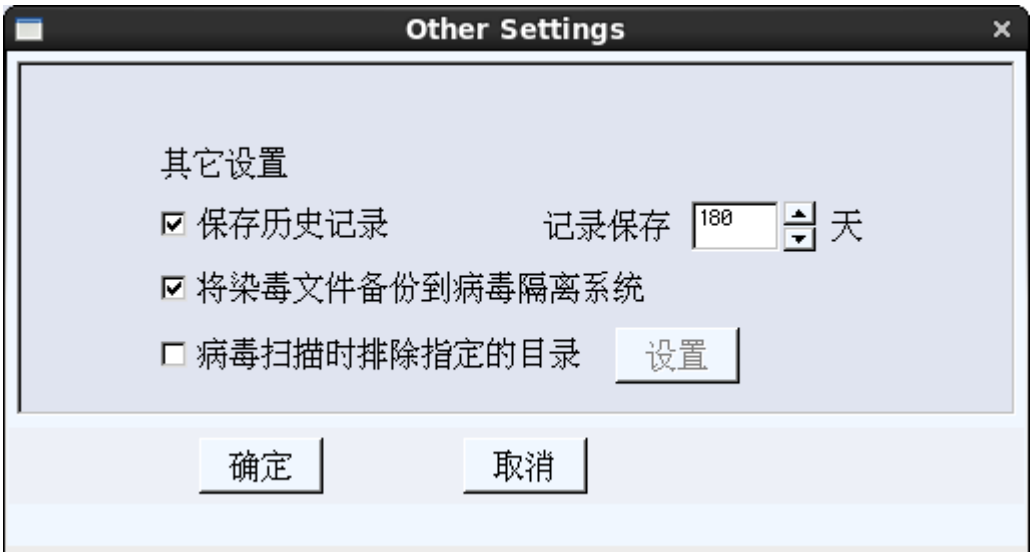
图表 4-173

在管理中心 URL 地址栏输入管理中心的地址和端口，点击【确定】。

4.7.1.2.6 其它设置

其他设置包括历史记录保存、病毒扫描排除目录、是否将备份感染分拣到隔离区。

在程序的主界面，选择菜单【设置】/【其他设置】，打开其他设置界面。

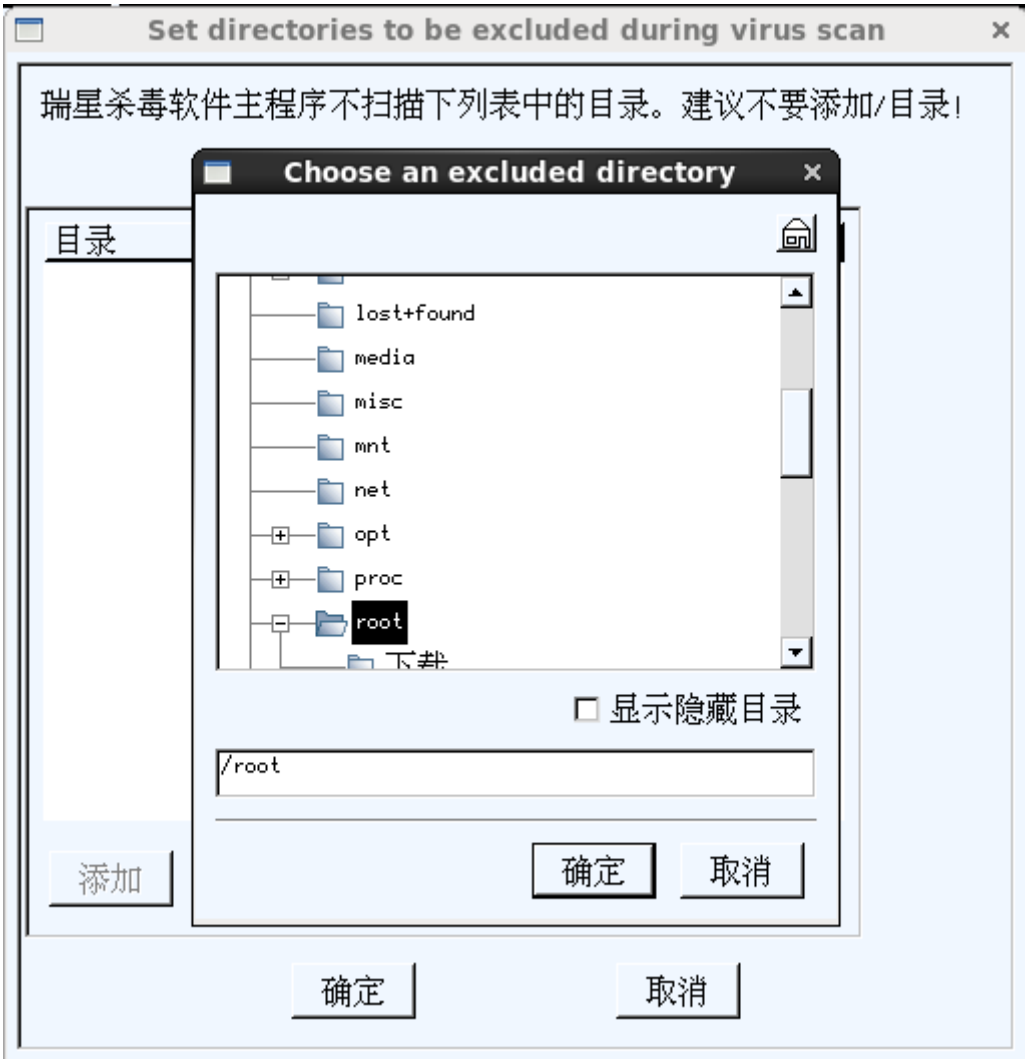


图表 4-174

【保存历史记录】：把用户扫描病毒的历史记录保存下来，便于以后在【操作】/【历史记录】中进行查看。勾选后，可设置保存记录的天数，最多可保存 365 天。

【将染毒文件备份到病毒隔离系统】：发现染毒文件时，先将其备份到病毒隔离系统，再对染毒文件进行处理。

【病毒扫描时排除指定的目录】：设定哪些目录在查杀病毒时不进行扫描。您可以点击【设置】打开添加窗口，添加一个或多个目录。建议不要添加/目录。



图表 4-175

4.7.2 管理中心远程扫描设置

详细请参考本文档章节 4.1.2.5.4.13 杀毒（Linux）。

4.8 Linux 全功能防护客户端

Linux 全功能防护客户端的设置包括系统设置和管理中心远程扫描设置两部分，分别对应客户端本地操作和管理中心远程扫描指令。

4.8.1 系统设置

“系统设置”是用户详细设置 Linux 全功能防护客户端的各功能界面，用户可在瑞星杀毒软件界面右上角点击“菜单”按钮。

图表 4-176

然后点击“系统设置”。

图表 4-177

之后就会打开“系统设置”的主界面，其中包括 “常规设置”、“查杀设置”、“可信文件”、“管理平台”和“其他设置”。

图表 4-178

4.8.1.1 常规设置

常规设置包括“自我保护”和“自动上传发现的可疑文件”两项设置。

4.8.1.1.1 自我保护

自我保护功能是为了避免木马病毒恶意篡改或删除瑞星杀毒软件程序组件（如未经授权修改瑞星杀毒软件的程序或尝试在其安装目录里面写入其他文件等），使客户计算机系统暴露于风险之中而设计，其默认为开启状态（项目被勾选）。

图表 4-179

注意：“自我保护”项目一直为开启状态，用户不能取消“自我保护”。

4.8.1.1.1.1 自我保护实例

安装完瑞星杀毒软件 for Linux 后，若尝试手动删除某个程序组件会失败

```
[root@redhat6 bin]# rm ravset
rm：是否删除普通文件 "ravset"？y
rm: 无法删除"ravset": 权限不够
```

图表 4-180

在“日志中心”的“防护日志”中会有尝试删除软件组件被阻止的记录。

图表 4-181

4.8.1.1.2 自动上传发现的可疑文件

“自动上传发现的可疑文件”是指在杀毒软件发现某个可疑文件，而本地病毒库中没有此文件特征，这时杀毒软件可将此文件上传到瑞星公有云安全服务器，依靠公有云的海量数据对此文件再次进行查杀，以进一步确保文件的安全性。

4.8.1.1.2.1 打开或关闭“自动上传发现的可疑文件”功能

用户可选择打开或关闭“自动上传发现的可疑文件”功能，此功能默认为开启状态（项目被勾选）。

图表 4-182

若用户想要关闭“自动上传发现的可疑文件”功能，可点击该项目前方勾选框，取消此项目的勾选状态。

图表 4-183

图表 4-184

然后点击页面右下方的“应用”按钮，这样就关闭了“自动上传发现的可疑文件”功能。

图表 4-185

若要再次打开该功能，用户只需再次勾选该项目，并点击“应用”即可。

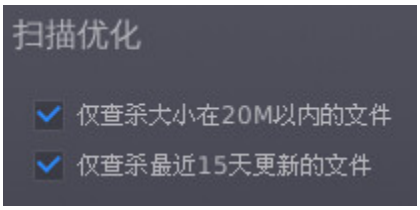
4.8.1.2 查杀设置

“查杀设置”是对木马病毒扫描的相关设置，包括 “扫描优化”和“扫描结果”两项内容，用户可在系统设置界面点击左列“查杀设置”来打开该界面。

图表 4-186

4.8.1.2.1 扫描优化

“扫描优化”是与木马病毒扫描相关的选项，包括“仅查杀大小在 20M 以内的文件”和“仅查杀最近 15 天更新的文件”。



图表 4-187

4.8.1.2.1.1 打开或关闭“仅查杀大小在 20M 以内的文件”功能

日常中我们碰到的绝大多数木马病毒，其大小均在 20M 以内，出于对查杀效率的考虑，瑞星杀毒软件 for Linux 默任开启此项功能。（项目被勾选）

图表 4-188

用户可选择关闭此项功能，点击该项目前的勾选框，取消其勾选状态。

图表 4-189

图表 4-190

然后点击页面右下方的“应用”按钮，这样就关闭了“仅查杀大小在 20M 以内的文件功能。

图表 4-191

关闭该功能后，杀毒软件将查杀 50M 大小以内的文件。若要再次打开该功能，用户只需再次勾选该项目，并点击“应用”即可。

4.8.1.2.1.2 打开或关闭“仅查杀最近 15 天更新的文件”功能

“仅查杀最近 15 天更新的文件”功能，是指杀毒软件只查杀 15 天内创建或修改的文件，这样做同样是出于对效率的考虑，该功能默认为开启状态。（项目被勾选）

图表 4-192

用户可选择关闭此项功能，点击该项目前的勾选框，取消其勾选状态。

图表 4-193

图表 4-194

然后点击页面右下方的“应用”按钮，这样就关闭了“仅查杀最近 15 天更新的文件”功能。

图表 4-195

关闭该功能后，杀毒软件将查杀任何时刻修改或创建的文件。若要再次打开该功能，用户只需再次勾选该项目，并点击“应用”即可。

4.8.1.2.2 扫描结果

“扫描结果”是设置发现病毒后如何进行处理的选项，包括“隔离病毒”、“用户选择处理”，或“忽略”。

图表 4-196

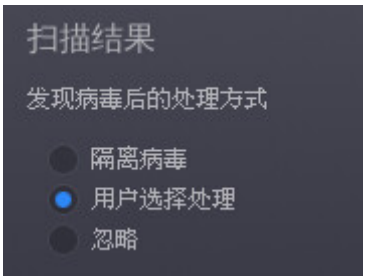
4.8.1.2.2.1 隔离恢复

“隔离恢复”是指杀毒软件在发现木马病毒后，对感染的文件进行清除或删除操作的同时，将感染文件复制到隔离区内，用户可在“日志中心”下的“隔离恢复”内看到被隔离的文件。“隔离病毒”是杀毒软件的默认选项。（选项钮为蓝色）

图表 4-197

4.8.1.2.2.2 用户选择处理

用户还可将扫描结果选择为“用户选择处理”（点击该项目前方选项钮）

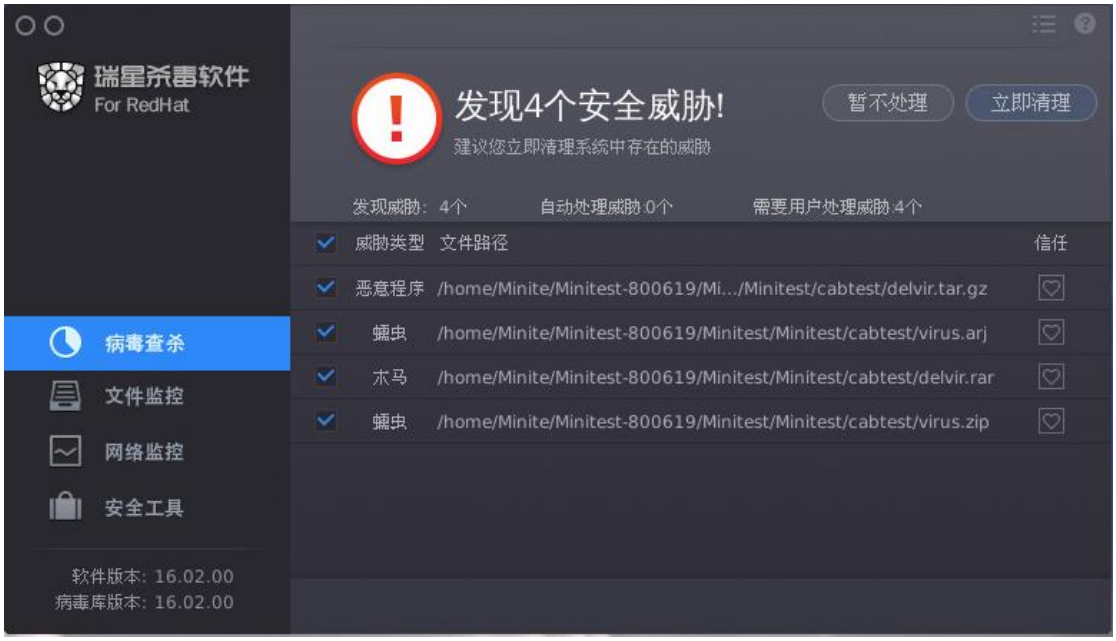


图表 4-198

之后点击页面右下角“应用”按钮使设置生效。

图表 4-199

之后用户再使用“病毒查杀”下任意一种查杀方式进行磁盘扫描，若发现木马病毒，在扫描结束后，将让用户选择是否处理这些病毒文件。（可选择“暂不处理”、“立即清理”或“信任”。）



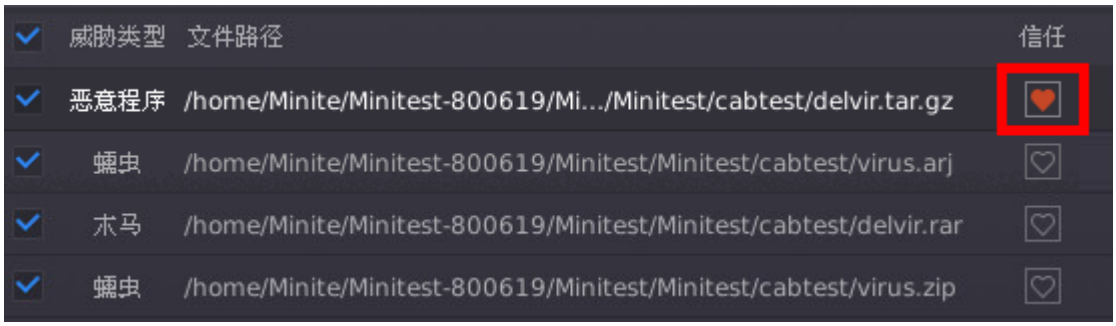
图表 4-200

若用户选择“暂不处理”

图表 4-201

则本次检查出的木马病毒均不会被清除或删除。

若用户点击被检查为木马病毒文件后的“信任”后，使该图标由灰色变为彩色。



图表 4-202

则当用户再次点击“立即清理”按钮后，被“信任”程序在本次不会被处理，其他未被“信任”的程序会被处理。

注意：此处的“信任”不要与加入“可信文件”列表的文件混淆，此处的“信任”是指本次扫描的结果为信任，下次扫描时，此程序还会被识别为木马病毒。

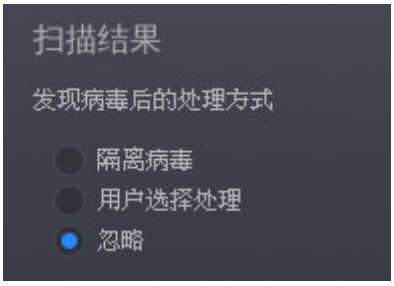
若用户选择“立即清理”。

图表 4-203

所有被查出的木马病毒均会被清除或删除。

4.8.1.2.2.3 忽略

用户还可将扫描结果选择为“忽略”（点击该项目前方选项钮）。

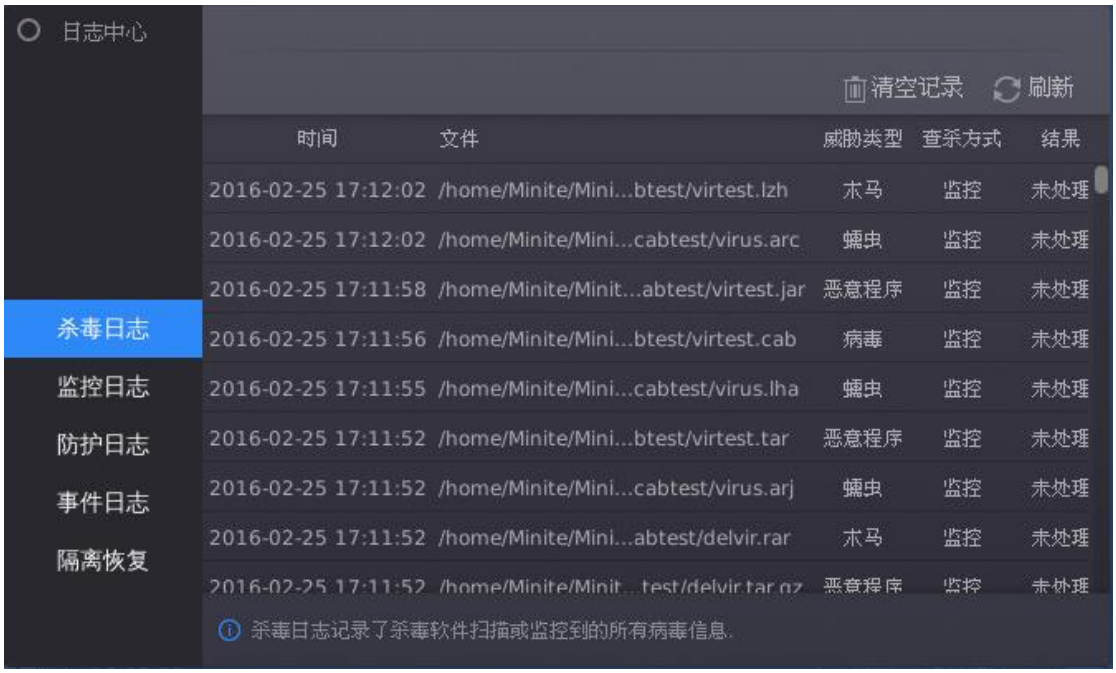


图表 4-204

之后点击页面右下角“应用”按钮使设置生效。

图表 4-205

当选择“忽略”时，杀毒软件在发现木马病毒后，将不会查杀病毒，而只会记录日志，用户可在“日志中心”的“杀毒日志”中看到这些记录，其“结果”为“未处理”。



图表 4-206

4.8.1.3 可信文件

“可信文件”即文件白名单，是指用户所添加的不希望被杀毒软件所查杀的文件，一旦文件或目录被添加到可信文件列表，无论其是否含有木马病毒，杀毒软件均不会对其进行查杀。

用户可在系统设置界面点击左列“可信文件”来打开该界面。

图表 4-207

4.8.1.3.1 添加或删除可信文件或可信目录

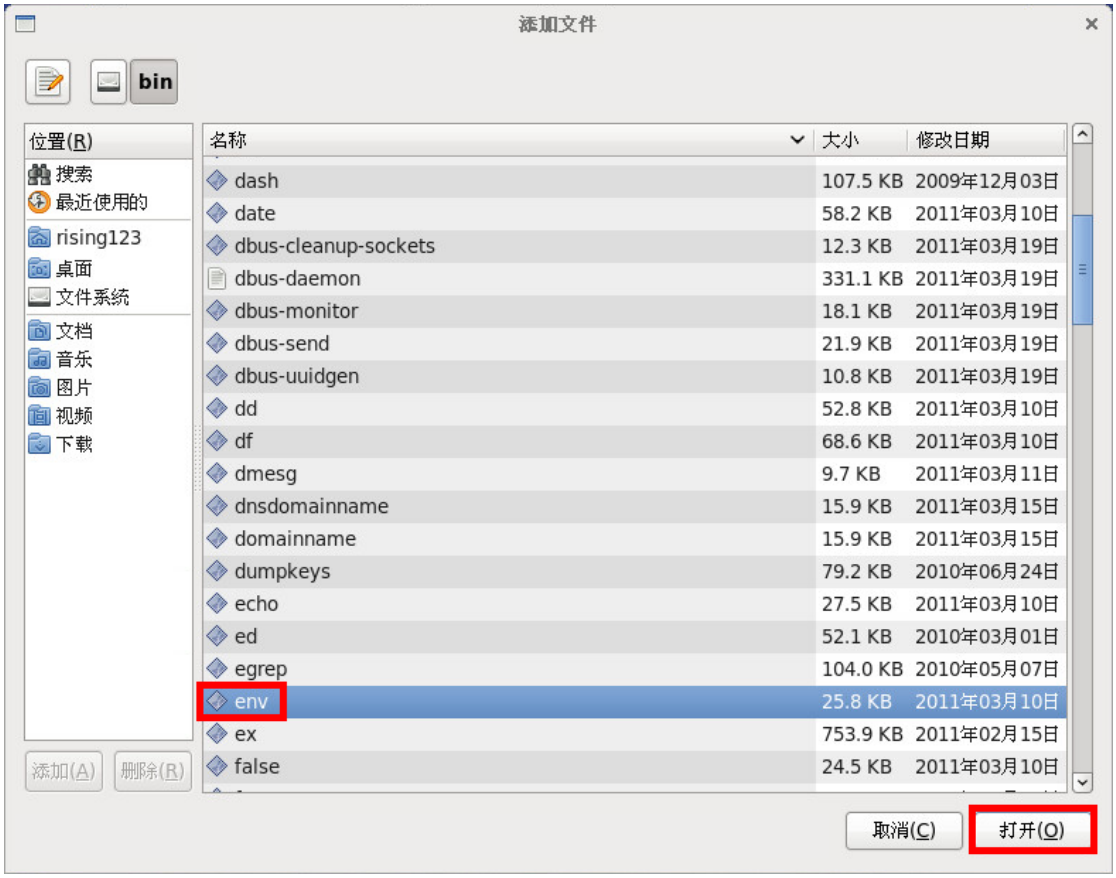
用户可在“可信文件”列表中添加或删除某个文件为可信文件，也可以添加或删除某个目录为可信目录。

4.8.1.3.1.1 添加某个可信文件

点击“可信文件”界面右上角的“添加”，选择“添加文件”。

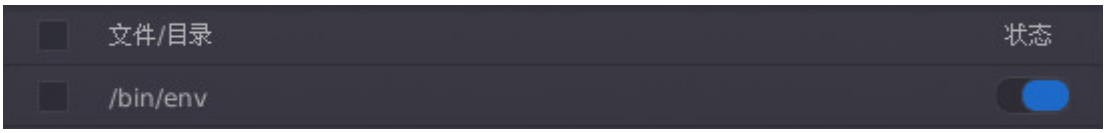
图表 4-208

打开文件浏览器，浏览并选择要添加到“可信文件”列表的文件，点击右下角“打开”。



图表 4-209

之后用户可在“可信文件”列表中看到刚添加的文件，且该项目的“状态”为打开，即文件可信（蓝色开关）。



图表 4-210

然后点击页面右下方的“确定”使设置生效。

图表 4-211

这样就完成了添加某个文件到“可信文件”列表当中。

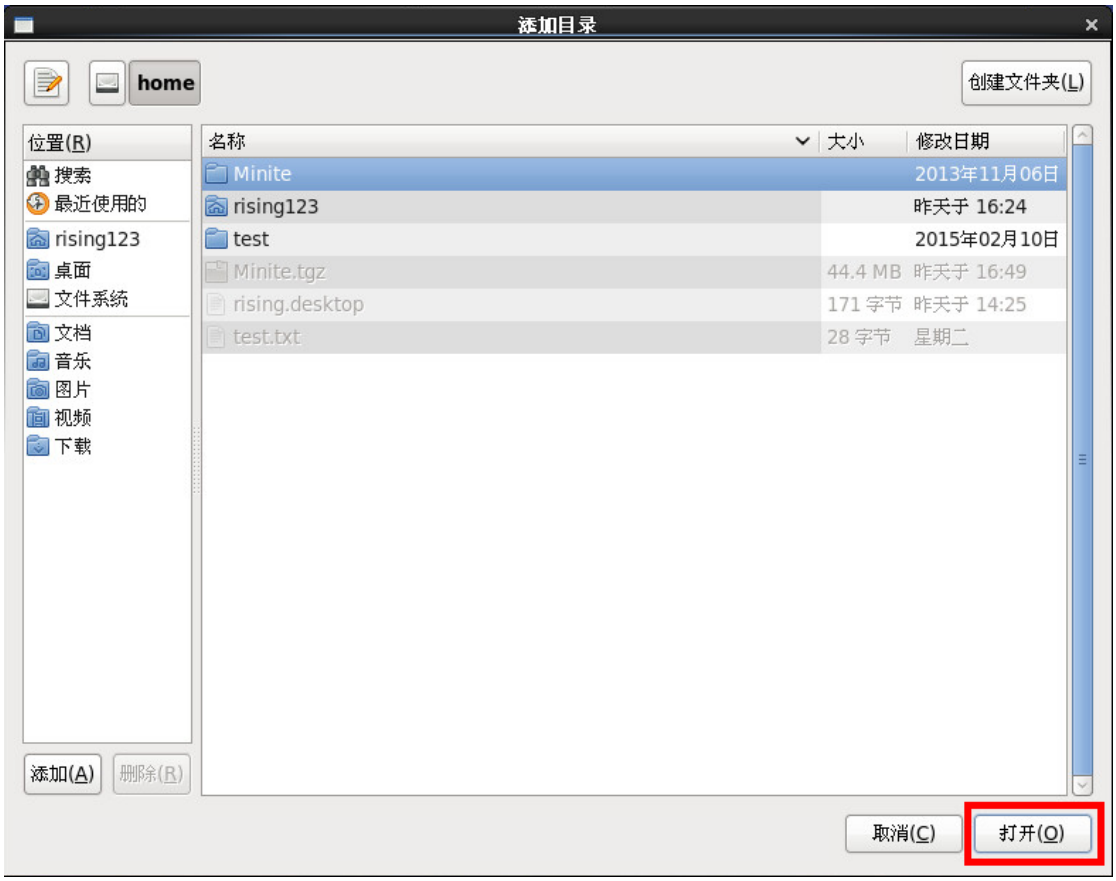
4.8.1.3.1.2 添加某个可信目录

除了添加某个文件外，用户还可以添加某个目录到可信文件列表，添加后，此目录下的所有文件都被当作“可信文件”处理。

点击“可信文件”界面右上角的“添加”，选择“添加目录”。

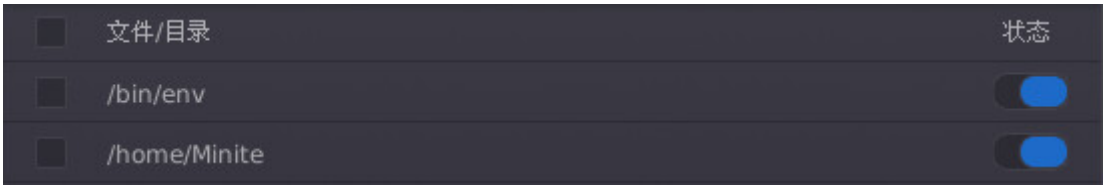
图表 4-212

打开文件浏览器，浏览并选择要添加到“可信文件”列表的目录，点击右下角“打开”。



图表 4-213

之后用户可在“可信文件”列表中看到刚添加的目录，且该项目的“状态”为打开，即目录可信（蓝色开关）。



图表 4-214

然后点击页面右下方的“确定”使设置生效。

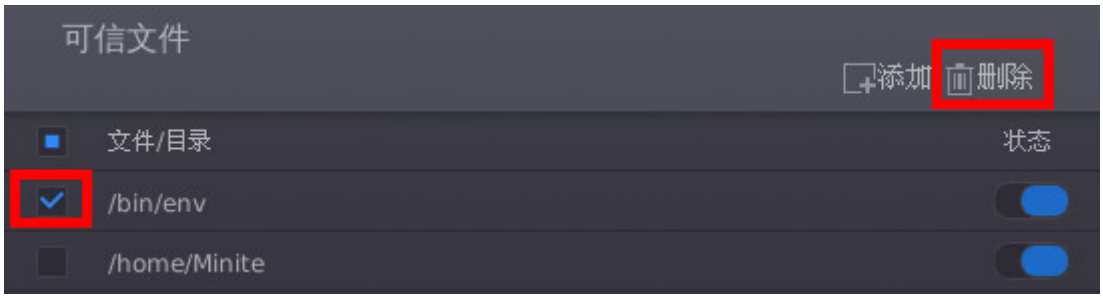
图表 4-215

这样就完成了添加某个目录到“可信文件”列表当中。

4.8.1.3.1.3 删除某个可信项目

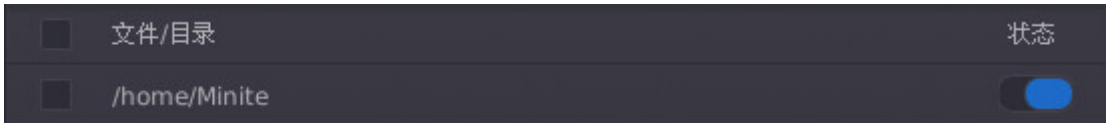
当“可信文件”列表中存在一个或多个项目时，用户可删除一个或多个可信项目，从列表中删除的文件或目录将不再作为“可信文件”，这些文件或目录会被杀毒软件进行检查。

在“可信文件”列表中勾选要删除的项目，点击右上角“删除”



图表 4-216

之后该项目在“可信文件”列表中消失。



图表 4-217

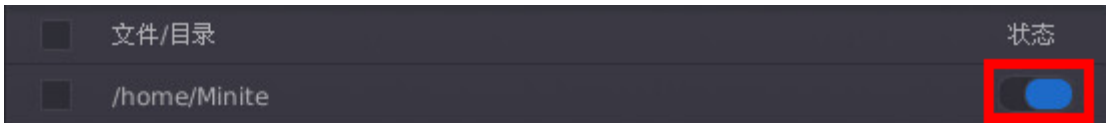
然后点击页面右下方的“确定”使设置生效。

图表 4-218

至此我们就删除了某个“可信文件”项目。

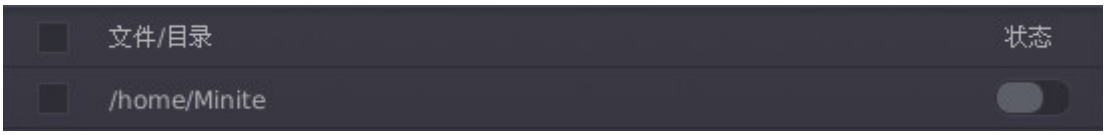
4.8.1.3.1.4 可信状态的开启及关闭

当“可信文件”列表中存在某可信文件或目录时，其“状态”默认为可信（蓝色开关），用户可点击该开关来改变其状态。



图表 4-219

之后该项目“状态”为关闭可信（灰色开关）。



图表 4-220

然后点击页面右下方的“确定”使设置生效，此时杀毒软件在碰到该项目时，会进行检查。

图表 4-221

4.8.1.3.2 可信状态实例

首先确认在“可信文件”列表中已经添加了某个文件或目录，并点击页面右下方“确定”使配置生效。（这里我们选择将某目录添加到“可信文件”列表，然后将病毒样本解压到此目录）。

图表 4-222

之后在“病毒查杀”功能的“自定义查杀”中，选择对该目录进行查杀，发现扫描结果没有任何病毒被扫出。

图表 4-223

这说明杀毒软件不会扫描添加到“可信文件”列表的项目。

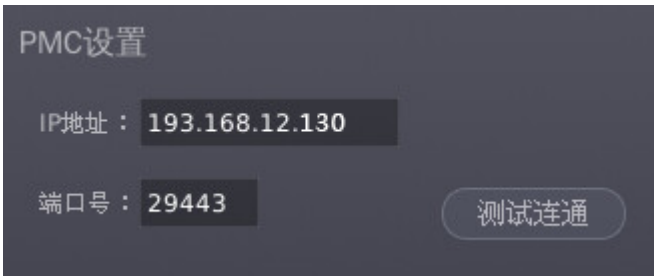
4.8.1.1 管理平台（PMC）

用户可在“系统设置”界面点击左侧“管理平台”来打开“管理平台”界面。

图表 4-224

4.8.1.1.1 输入管理平台 IP 地址及端口

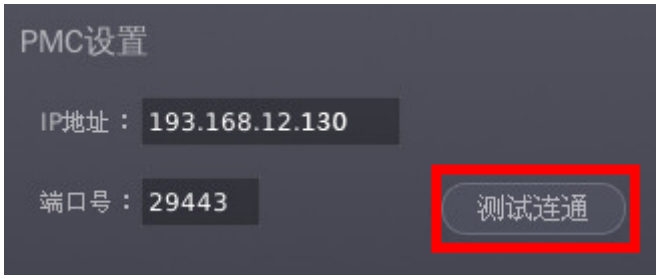
用户可以在“管理平台”界面将填入“管理平台”的 IP 地址及端口信息。



图表 4-225

4.8.1.1.2 测试连通性

当用户输入了“管理平台”的 IP 地址及端口后，建议用户点击“测试连通”按钮确认是否可成功连接到“管理平台”。



图表 4-226

如果不能连接到“管理平台”，软件会提示“连接测试失败”。

图表 4-227

用户可再次检查输入的“管理平台”IP 地址及端口是否正确，如果已经正确，请排查网络问题，正常情况下，用户点击“测试连通”按钮后会显示“连接测试成功”。

图表 4-228

如果设置的 IP 地址和端口可以正确连接到“管理平台”，点击页面右下方的“确定”按钮使设置生效。

图表 4-229

至此就完成了将此客户端连接到“管理平台”，管理员可从“管理平台”（PMC）上管理此客户端。

4.8.1.2 其他设置

用户可在“系统设置”的界面点击左列“其他设置”打开该设置界面，此界面主要包括“日

志清理”。

图表 4-230

“日志清理”中有一个选项“根据日志类型自动智能清理”，该选项默认勾选，且用户不能取消其勾选状态。该选项的功能是“监控日志”或“防护日志”中的日志大于 1000 条时，杀毒软件将优先从第 1 条开始清理（删除掉旧的日志），清理根据日志存取时间，优先清理时间早的日志，但每次清理不会大于 500 条。

4.8.1.3 恢复默认设置

在“系统设置”界面的下部，有个“恢复默认设置”按钮。

图表 4-231

当用户点击“恢复默认设置”，并点击页面下方的“确定”按钮后，所有各项设置恢复到软件安装后的默认状态。

图表 4-232

4.8.2 管理中心远程扫描设置

详细请参考本文档章节 4.1.2.5.4.14 杀毒&防火墙（Linux）。

5 安全功能

5.1 VMware 无代理杀毒

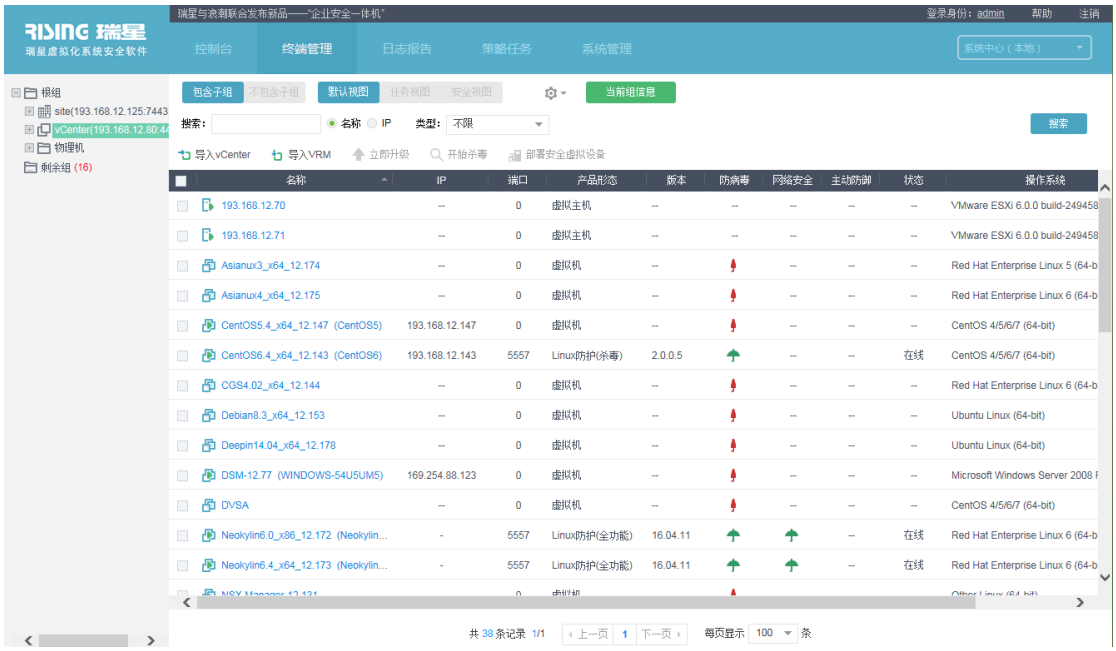
5.1.1 手动查杀

请按照下面的步骤完成操作：

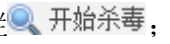
第一步：启动并登录瑞星虚拟化系统安全软件管理中心控制台；

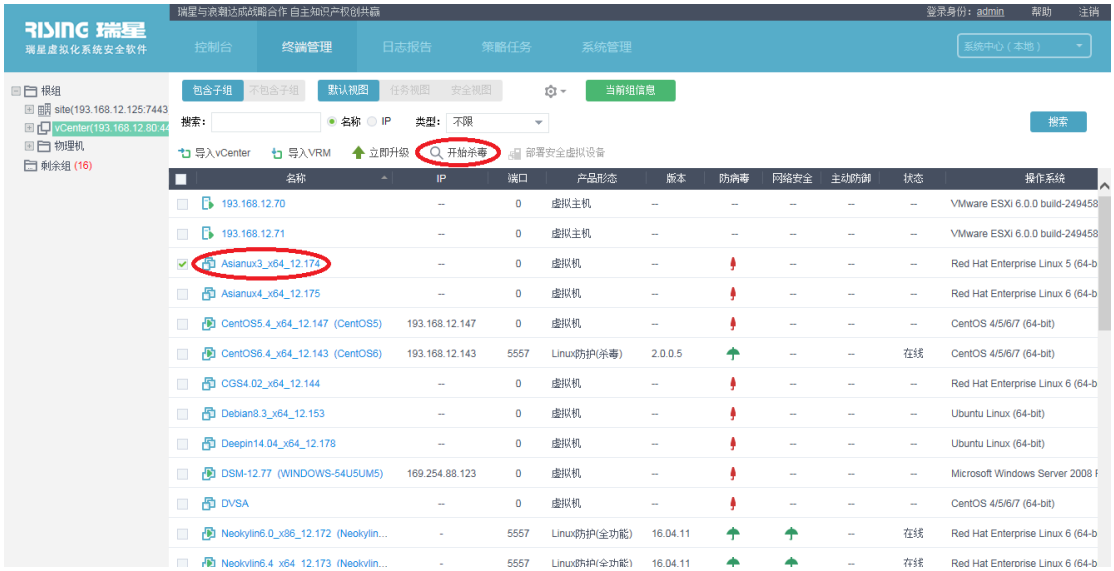
图表 5-1

第二步：切换到【终端管理】标签页，点击【vCenter】组，显示所有被管理的 VMware 终端；



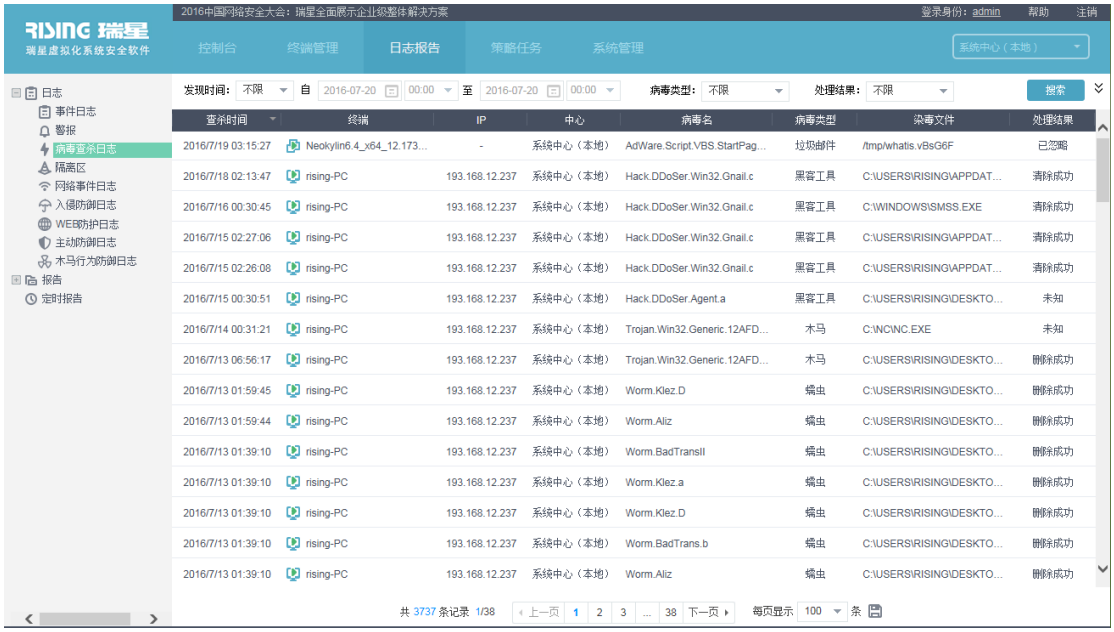
图表 5-2

第三步：勾选需要查杀的虚拟机终端，点击工具栏  ；



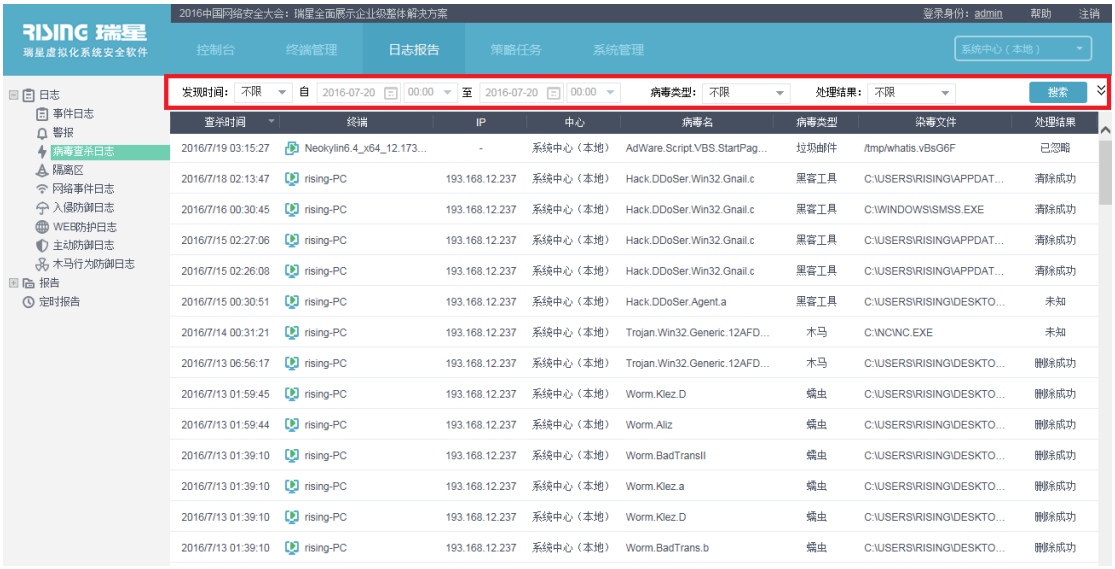
图表 5-3

第四步：当查杀病毒时，点击【病毒查杀日志】，实时查看查杀记录；



图表 5-4

第五步：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。



图表 5-5

查杀策略设置请参考本文档章节 4.1.4.1.1 扫描策略。

5.1.2 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病毒查杀日志窗口会列出相应的病毒查杀记录信息。 病毒查杀日志窗口请参考本文档章节 4.1.3.1.2 病毒查杀日志。

文件监控策略设置请参考本文档章节 4.1.4.1.2 文件监控策略。

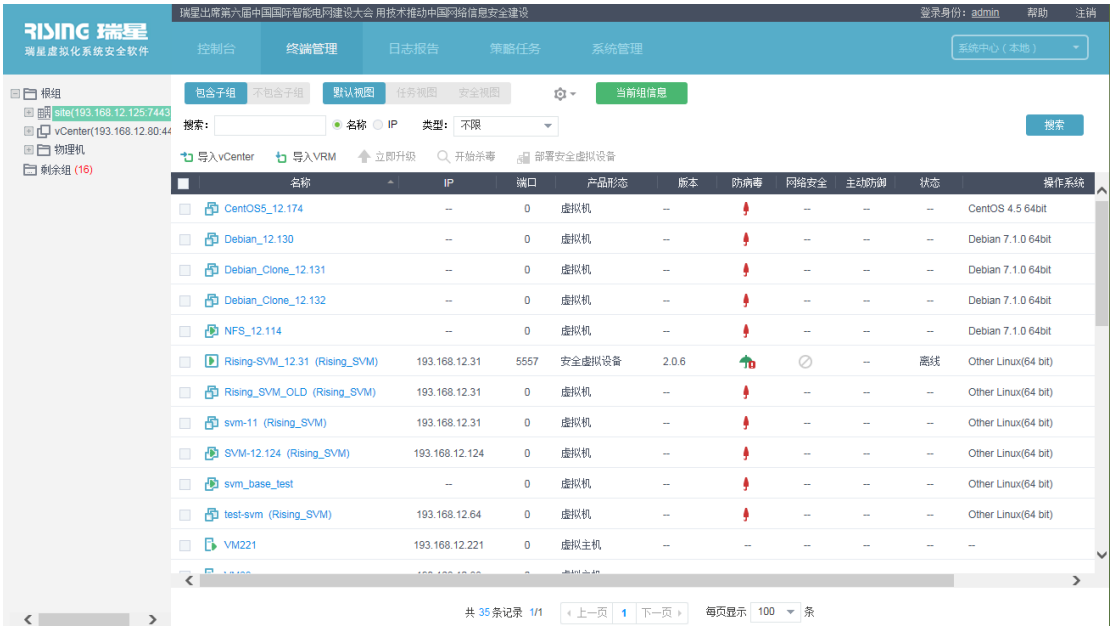
5.2 HUAWEI 无代理杀毒

5.2.1 手动查杀

手动查杀请参考本文档章节 5.1.1 手动查杀。

其中，第二步做如下修改。

第二步：切换到【终端管理】标签页，点击【site】组，显示所有被管理的 VRM 终端；



图表 5-6

5.2.2 文件监控

文件监控请参考本文档章节 5.1.2 文件监控。

5.2.3 防火墙功能

HUAWEI 无代理杀毒的防火墙功能，通过管理中心向 HUAWEI 无代理杀毒下发策略实现防火墙的相关配置。

防火墙功能的策略设置请参考本文档章节 4.1.2.5.3.3 防火墙（Huawei）、4.1.2.5.3.4 IP 黑白名单（Huawei）、4.1.2.5.3.5 入侵防御（Huawei）、4.1.2.5.3.6 WEB 信誉（Huawei）、4.1.2.5.3.7 VPatch（Huawei）。

5.3 安全防护终端

安全防护终端提供有代理部署场景下的 Windows 系统安全防护功能，支持使用病毒查杀设置执行本地查杀和远程扫描指令，并能够实现本地实时监控、主动防御等高级防护，处理结果以日志形式统一上报管理中心。

5.3.1 病毒防护

5.3.1.1 本地查杀

5.3.1.1.1 手动查杀

操作方法：

第一步：启动瑞星虚拟化系统安全软件安全防护终端，单击【杀毒】标签页。

第二步：确定要扫描的文件夹或者其它目标，在【查杀目标】中被勾选的目录即是当前选定的查杀目标。

第三步：单击【开始查杀】，则开始查杀相应目标，发现病毒立即清除；扫描过程中可随时单击【暂停查杀】按钮来暂时停止查杀病毒，按【继续查杀】按钮则继续查杀，或单击【停止查杀】按钮停止查杀病毒。查杀病毒过程中，文件数、病毒数和查杀百分比将显示在下面，并且可以通过【详细信息】查看查杀病毒的详细情况，其中包括：当前查杀文件路径、查杀信息、查杀进度、病毒列表等。若瑞星虚拟化系统安全软件安全防护终端发现病毒，则会将文件名、所在文件夹、病毒名称和状态显示在此窗口中。在每个文件名称前面有图标标明病毒类型，病毒类型详见识别病毒类型。通过【概要信息】返回到前一页面。另外，查杀病毒方式可以使用右键菜单对染毒文件进行处理。

第四步：查杀结束后，扫描结果将自动保存到工作目录的指定文件中，可以通过历史记录来查看以往的查杀病毒结果。

第五步：如果想继续查杀其它文件或磁盘，重复第二、第三步即可。

图表 5-7

5.3.1.1.2 空闲时段查杀

空闲时段查杀可以利用用户的闲暇时间扫描电脑中的文件。用户可以启用屏保查杀，当电脑处于屏幕保护状态时，瑞星虚拟化系统安全软件安全防护终端会对指定的文件进行扫描，有效利用时间。用户还可以设置定时任务，指定自己的空闲时间进行查杀任务。

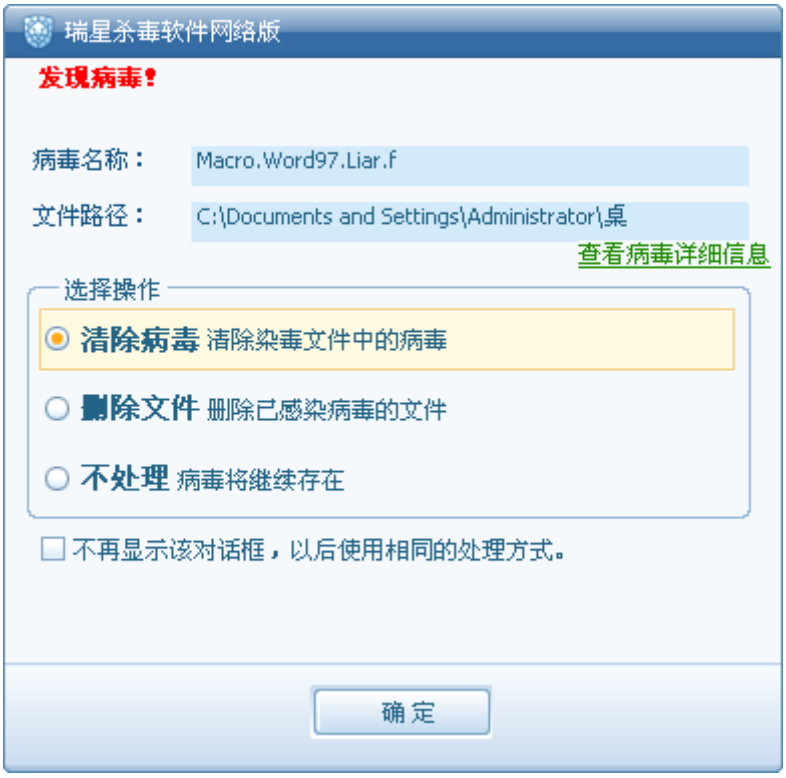
当空闲时段查杀启动后，在桌面右下角会出现瑞星图标，双击此图标可弹出空闲时段查杀页面，在此页面中用户可以查看查杀详细信息。

图表 5-8

5.3.1.1.3 嵌入式查杀

瑞星虚拟化系统安全软件安全防护终端支持对 Office/IE、Outlook 进行嵌入式杀毒，同时也支持一些其它工具的嵌入式杀毒。每次用户接收发邮件时候，瑞星虚拟化系统安全软件安全防护终端可以对邮件进行病毒查杀，保障邮件安全；当打开 Office 文档时或者用 IE 下载插件程序文件时，Office/IE 嵌入式杀毒可以自动扫描病毒；当使用 MSN 收发文件时候，瑞星虚拟化系统安全软件安全防护终端可以检查文件是否携带病毒等等。

下面举例，如果启动的 Office 2000 文件中有病毒存在，会自动弹出提示对话框。用户可以根据需要选择相应的操作，如【清除病毒】、【删除文件】和【不处理】。如果清除病毒失败，会提供清除失败后的处理方式供用户选择。



图表 5-9

5.3.1.2 远程扫描

详细请参考本文档章节 5.1.1 手动查杀。

5.3.1.3 实时监控

5.3.1.3.1 文件监控

文件监控用于实时的监控系统中的文件操作，在操作系统对文件操作之前对文件查毒，从而阻止病毒运行，保护系统安全。

文件监控在工作中发现病毒时，会对用户进行提示：用户可以选择【清除病毒】、【删除文件】或【不处理】。如果超过一定时间用户没有做出选择，那么文件监控将会对此病毒采取当前选择的处理方式。

图表 5-10

超时文件提示：当文件监控在查杀大容量压缩文件时，会占用较多的系统资源，造成系统效率降低。瑞星虚拟化系统安全软件安全防护终端的文件监控，在遇到此类情况时能够提示用户进行操作。用户可以在提示的对话框中选择跳过对该文件的查杀，避免文件监控长时间占用系统资源，减少对系统的影响。

5.3.1.3.2 邮件监控

用户在接收或发送邮件时，邮件监控可以对接收和发送的邮件进行病毒扫描，防止病毒通过邮件传播，感染电脑。

邮件监控功能支持所有符合 SMTP 和 POP3 协议的邮件客户端，如 Foxmail 和 Outlook 等。

- POP3 协议：规定如何将个人电脑连接到 Internet 的邮件服务器，以及在下载电子邮件时允许用户从服务器上把邮件存储到本电脑，同时删除保存在邮件服务器上的邮件。

- SMTP 协议： SMTP 协议属于 TCP/IP 协议族,它帮助电脑在发送或中转邮件时找到下一个目的地。通过 SMTP 协议所指定的服务器，就可以把邮件发送到对方服务器，整个过程只要几分钟。

当用户选择发送和接收邮件的时候，邮件监控会自动进行扫描工作。此时，如果用户在【设置】/【监控设置】/【邮件监控】的高级设置选项页面中，取消勾选【隐藏瑞星邮件收发进度提示】将显示发送或接收邮件的进度，如图：

图表 5-11

发送和接收的邮件中，当有程序触发邮件监控的时候，会显示以下界面提示用户发现病毒，为用户提供处理病毒的操作方式，分别为【清除病毒】、【删除附件】和【不处理】，或者设定时间到达后按当前选择的处理方式。如图：

图表 5-12

5.3.1.4 智能主动防御

5.3.1.4.1 系统加固

智能主动防御是一种阻止恶意程序执行的技术。瑞星的主动防御技术提供了更开放的高级用户自定义规则的功能，用户可以根据自己系统的特殊情况，制定独特的防御规则，使主动防御可以最大限度的保护系统。

智能主动防御功能设计脱离了病毒库，以往只是发现应用程序类似病毒就去病毒库中进行验证，这样判断病毒都是已经发现的病毒，对于新病毒便失去了防御作用。主动防御具有独特的功能设计，它是瑞星公司根据多年判断病毒的经验制定了一系列的规则，通过规则过滤应用程序，当发现其存在恶意行为的时候，便告知用户，这样将处理此恶意行为的权力交给用户，由用户决定放过还是拒绝此类危险动作，从而可以达到主动预防病毒的作用。即使遇到一个病毒库里面没有记录的新病毒，也可以提前帮助用户发现它。在病毒肆虐的网络中，

主动防御功能在病毒与计算机之间又设置了一道屏障，将病毒置之门外。

主动防御由系统加固、应用程序控制、木马行为防御、木马入侵拦截（U 盘拦截）、木马入侵拦截（网站拦截）和自我保护等功能组成。

选择瑞星虚拟化系统安全软件安全防护终端主界面的防御界面，可以开启和设置主动防御的各项功能，如图：

图表 5-13

注：所有64位操作系统不支持主动防御功能。

5.3.1.4.2 应用程序控制

系统加固针对恶意程序容易利用的操作系统脆弱点进行监控、加固，以抵御恶意程序对系统的侵害。系统加固为用户预先设置了规则，并提供规则的应用对象，这些规则对象主要由容易被病毒利用的操作系统脆弱点构成，并且针对对象是否启用规则，为用户量身制定了高、中、低、自定义四种安全级别，由用户根据系统情况自由选择。

系统加固对系统动作、注册表、关键进程和系统文件进行监控，从而防止恶意程序对操

作系统进行修改系统进程，操作注册表，破坏关键进程和系统文件等危险行为。

说明：系统加固功能中的规则范围是瑞星虚拟化系统安全软件安全防护终端设置的，用户无法添加或者删除，但可以设置是否启用系统加固的各项规则。用户可以使用瑞星软件默认的使用级别，也可以对其进行设置。

在瑞星虚拟化系统安全软件安全防护终端主界面中选择防御页面中的系统加固，设置状态为开启，系统加固规则主要有四种类型，下面对触发这四种类型的规则的情况分别举例。

第一种类型：触发系统监控规则

当有程序触发全局挂钩规则，会弹出包含简要信息的对话框、和触发的规则信息，如图：

图表 5-14

第二种类型：触发注册表规则

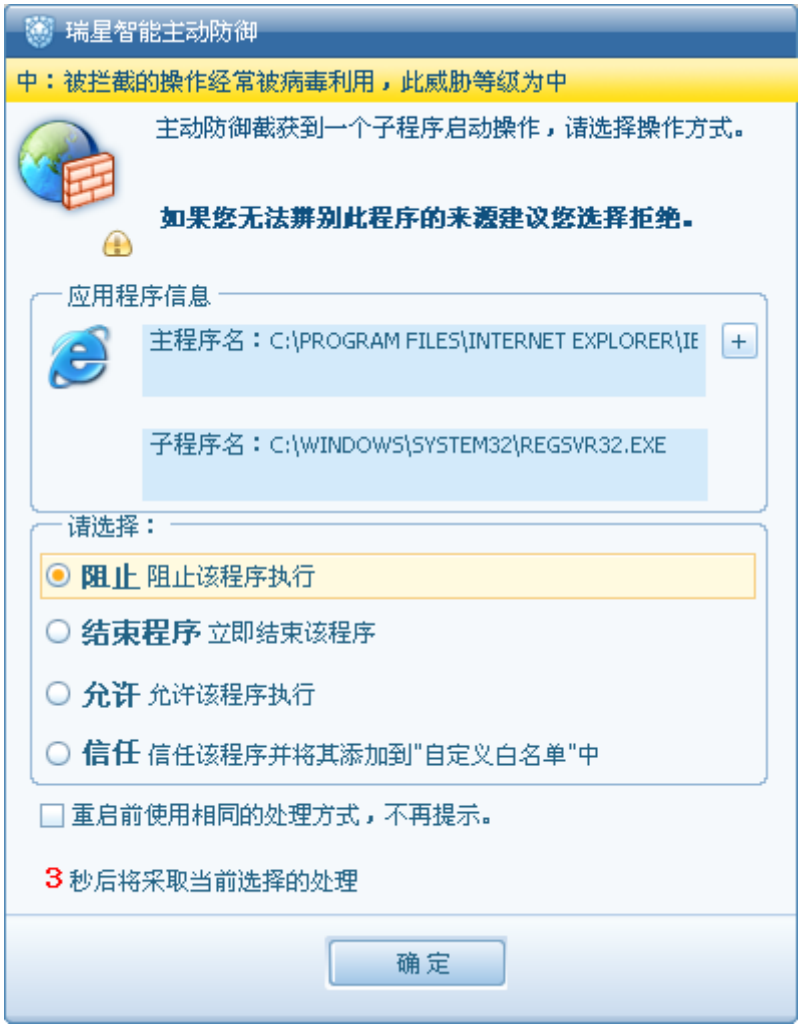
当有程序触发注册表规则的时候，提示用户信息对话框如图。用户可以根据提示选项选

择处理结果。

图表 5-15

第三种类型：触发启动子进程规则

当 IE 启动子进程时候，提示用户信息对话框如图。用户可以根据提示选项选择处理结果。



图表 5-16

第四种类型：触发系统文件规则

当有程序触发操作系统文件规则的时候，提示用户信息对话框如图。用户可以根据提示选项选择处理结果。

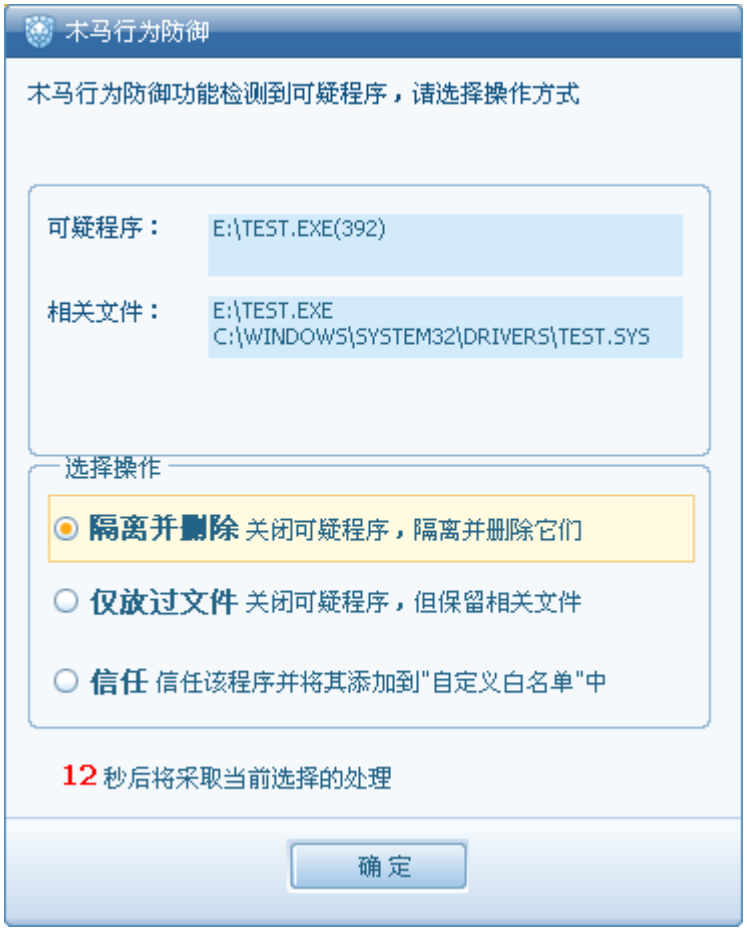
图表 5-17

5.3.1.4.3 木马行为防御

通过对木马等病毒的行为分析，智能监控未知木马等病毒，抢先阻止其偷窃和破坏行为。

说明：此功能是瑞星虚拟化系统安全软件安全防护终端提供内置规则，用户可以进行相关设置，当此功能开启的时，木马行为防御功能生效。如何设置请参考 4.4.1.2.3 木马行为防御设置。

若用户设置为发现恶意行为后的处理方法为【提示我处理】时，则会提示用户处理此程序。如图：



图表 5-18

5.3.1.4.4 木马入侵拦截（U 盘拦截）

通过对木马病毒传播行为的分析，阻止其通过 U 盘、光盘等入侵用户电脑，阻断其利用存储介质传播的通道。

木马入侵拦截（U 盘拦截）取代了原来的 U 盘监控，控制范围更广，能够更好地控制执行区域，避免外部病毒感染到主机。当木马入侵拦截（U 盘拦截）范围内的程序试图自动运行或直接运行的时候，进行拦截，并提示用户。

下面举例，当有移动磁盘上有程序执行时候，提示信息如下，用户可根据建议或者实际情况决定是否允许程序执行。

图表 5-19

5.3.1.4.5 木马入侵拦截（网站拦截）

通过对恶意网页行为的监控，阻止木马病毒通过网站入侵用户电脑，将木马病毒威胁拦截在电脑之外。

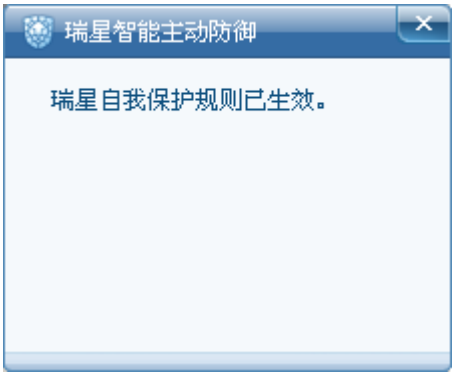
木马入侵拦截(网站拦截)突破了原来网页脚本扫描只能通过特征进行查杀的技术壁垒，解决了原网页脚本监控无法对加密变形的病毒脚本进行处理的问题。由于采用的是行为检测查杀，对于网页挂马一类的木马有很好的防御和处理能力。

当有程序触发木马入侵拦截（网站拦截）时候，会有如下提示，用户可根据情况选择是否允许执行。

图表 5-20

5.3.1.4.6 自我保护

瑞星虚拟化系统安全软件安全防护终端提供自我保护功能，防止恶意程序破坏瑞星虚拟化系统安全软件安全防护终端。如果有破坏瑞星虚拟化系统安全软件安全防护终端的情况出现，电脑右下方会有相应提示。如图：



图表 5-21

5.3.2 网络监控

恶意网址拦截、网络攻击拦截、出站攻击拦截、访问控制、IP 包过滤功能是被动功能，

当触发设置的规则和功能后，安全防护终端将通过软件提示或者是右下角的弹窗提示拦截信息和处理方式，用户选择相应的处理方式。

5.3.3 工具

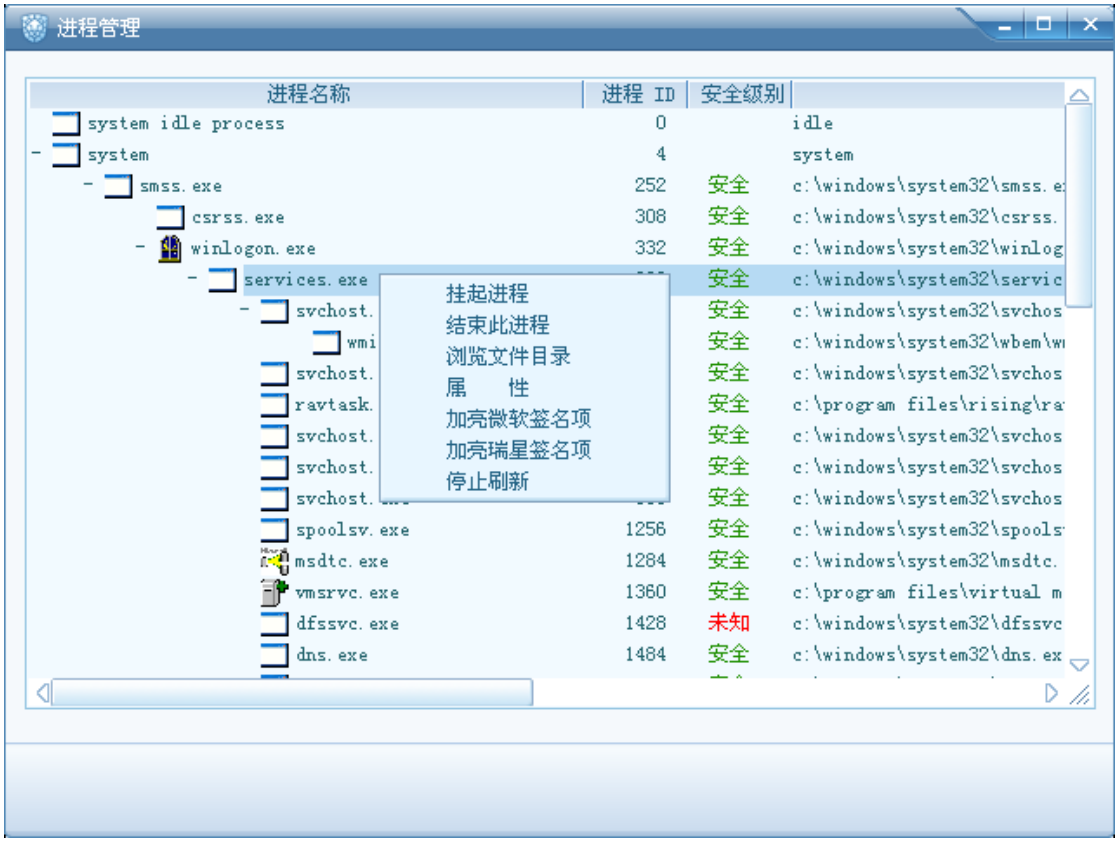
5.3.3.1 网络连接

单击瑞星虚拟化系统安全软件安全防护终端主程序【工具】标签页，单击对应【网络连接】的【运行】链接，打开网络连接查看当前网络连接状态。用户可以右键选择【全部展开】或启用/停止刷新。

图表 5-22

5.3.3.2 进程信息

单击瑞星虚拟化系统安全软件安全防护终端主程序【工具】标签页，单击对应【进程信息】的【运行】链接，查看当前进程信息。



图表 5-23

用户可以选中进程后，右键选择对进程的各种操作选项：

挂起进程：挂起选中的进程。

结束此进程：结束选中的进程。

浏览文件目录：打开进程所在的目录进行浏览。

属性：选择该菜单项则查看进程属性。

可疑文件上报：将选中的可疑文件上报。

加亮微软签名项：将微软签名程序加亮显示。

加亮瑞星签名项：将瑞星签名程序加亮显示。

停止/自动刷新：停止或者刷新当前进程信息。

5.3.3.3 嵌入式杀毒设置

瑞星虚拟化系统安全软件安全防护终端嵌入式杀毒工具是在用户使用即时通讯软件（如

MSN Messenger）、压缩工具（如 WinZip）和下载工具（如 FlashGet）时，会自动调用瑞星虚拟化系统安全软件安全防护终端对接收的文件进行病毒扫描，防止病毒感染您的电脑。

瑞星虚拟化系统安全软件安全防护终端嵌入式杀毒工具目前支持的软件有：

MSN Messenger

AOL Messenger

FlashGet

NetVampire

WinZip

WellGet

WinRAR

FlashGet 2

操作方法：

打开嵌入式杀毒设置对话框

方法一：在瑞星虚拟化系统安全软件安全防护终端主程序界面中，选择【工具】 / 【嵌入式杀毒设置】 / 【运行】

方法二：在 Windows 画面中，选择【开始】 / 【所有程序】 / 【瑞星虚拟化系统安全软件】 / 【瑞星工具】 / 【嵌入式杀毒设置】

用户可以选中软件图标，点击【开启】或【关闭】按钮打开或关闭嵌入式杀毒功能。

图表 5-24

在支持软件的列表中，列出了已经安装的软件，开启嵌入式杀毒支持的软件后，则当这些软件在接收文件后会自动调用瑞星虚拟化系统安全软件安全防护终端扫描病毒。

5.3.3.4 病毒隔离区

病毒隔离系统将安全隔离并保存染毒文件的备份，用户可以从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。

启动病毒隔离系统

方法一：在瑞星虚拟化系统安全软件安全防护终端主程序界面中，选择【工具】/【病毒隔离区】/【运行】。

方法二：在 Windows 画面中，选择【开始】/【程序】/【瑞星虚拟化系统安全软件】/【病毒隔离区】。

注意： 如果用户在瑞星虚拟化系统安全软件安全防护终端主程序界面中，选择【设置】/【详细设置】/【其它设置】，在设置页面中勾选【将染毒文件备份到病毒隔离区】，则病毒隔离系统将保存染毒文件的备份，并且在必要时，用户可以恢复备份的染毒文件副本。

图表 5-25

操作选项：操作（恢复、恢复为、删除、清空、关闭病毒隔离区）

选择选项：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、被相同病毒感染的文件

查看选项：刷新列表、查看病毒资料、排列项目（按日期、按名称、按路径、按大小）

工具选项：设置空间

帮助选项：帮助、关于病毒隔离区

针对被隔离的文件的操作：（右键操作）恢复、恢复为、删除、全部选定、反向选择、选中相同时间的文件、选中相同路径的文件、选中被相同病毒感染的文件、查看病毒资料。

为避免由于备份文件过多而占用大量磁盘空间，用户可以设置病毒隔离系统占用存储空间的大小。当隔离区空间已满时，用户可以选择【空间自动增长】或使用【替换最老的文件】处理。方法是：启动【病毒隔离区】，选择【工具】/【设置空间】，在【设置】对话框中选择后，再按【确认】保存设置。

5.4全功能安全防护客户端

全功能安全防护客户端支持使用客户端设置执行本地查杀，而且能够接收管理中心下发策略进行远程扫描，处理结果以日志形式统一上报管理中心。

主要功能包括病毒查杀、系统防护、网络防护、上网管理和安全日志。

5.4.1 病毒查杀

病毒查杀分为全盘查杀和自定义查杀。

图表 5-26

5.4.1.1 全盘查杀

单击【快速查杀】下拉菜单，单击【全盘查杀】：

图表 5-27

进入全盘查杀页面，开始全盘查杀，包括系统引导区、系统目录、系统内存、桌面文件、自启动程序、系统磁盘。

图表 5-28

全盘查杀完成后，显示查杀结果：

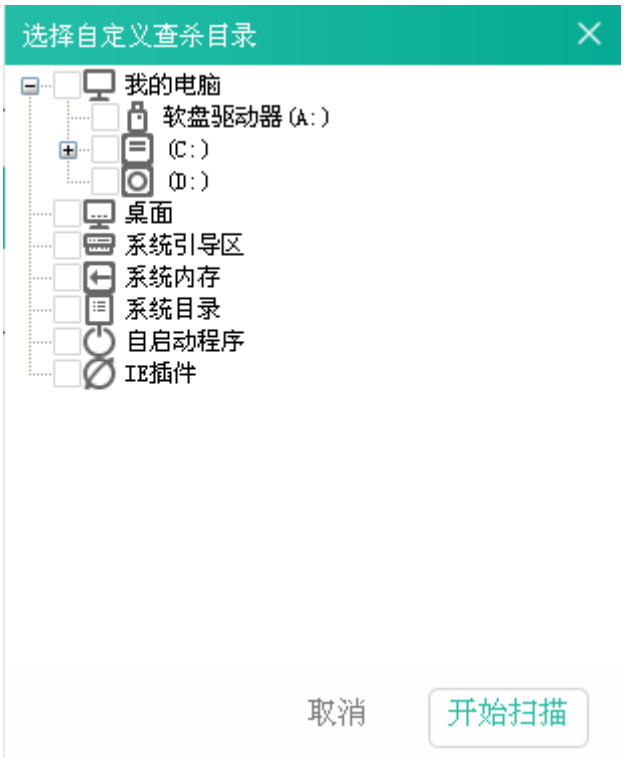
图表 5-29

5.4.1.2 自定义查杀

单击【快速查杀】下拉菜单，单击【自定义查杀】：

图表 5-30

进入自定义查杀页面，选择自定义查杀目录，单击 开始扫描 ，进行自定义查杀。



图表 5-31

5.4.1.3 隔离区

单击【病毒查杀】页面的 隔离区(0)，进入已隔离页面，对于已隔离的文件，可以恢复到原始位置、恢复到指定位置或删除。

图表 5-32

5.4.2 系统防护

系统防护包括文件监控、内核监控和 U 盘防护。

图表 5-33

5.4.2.1 文件监控

单击【文件监控】，进入文件监控页面，可以选择监控等级、文件类型、优化选项、病毒处理和是否记录日志。

图表 5-34

5.4.2.2 内核监控

单击【内核监控】，进入内核监控页面，可以进行系统加固设置、完整性监控、报警方

式和是否记录日志。

图表 5-35

5.4.2.3 U 盘防护

单击【U 盘防护】，进入 U 盘防护页面，可以设置 U 盘防护和是否记录日志。

图表 5-36

5.4.3 网络防护

网络防护包括 IDS/IPS、Vpatch、WEB 信誉、阻止攻击和敏感词审查。

图表 5-37

5.4.3.1 IDS/IPS

IDS/IPS 功能监测并阻止黑客或病毒对本系统发起的网络攻击。单击【IDS/IPS】，进入 IDS/IPS 页面，可以设置 IDS/IPS 专家规则库、报警方式、是否记录日志和 SQL 防注入。

图表 5-38

5.4.3.2 Vpatch

Vpatch 功能避免系统因 0Day 漏洞而遭受网络攻击。单击【Vpatch】，进入 Vpatch 页面，可以设置 IDS/IPS 专家规则库、报警方式、是否记录日志和 SQL 防注入。

图表 5-39

5.4.3.3 WEB 信誉

WEB 信誉自动拦截网页木马攻击及钓鱼欺诈网站。单击【WEB 信誉】，进入 WEB 信誉页面，可以选择需要防护的浏览器、是否记录日志、白名单和黑名单。

图表 5-40

5.4.3.4 阻止攻击

阻止攻击功能阻止本系统因病毒入侵而对其他网络设备发起攻击行为。单击【阻止攻击】，进入阻止攻击页面，可以设置阻止对外攻击、报警方式和是否记录日志。

图表 5-41

5.4.3.5 敏感词审查

敏感词审查功能监控并阻止通过网页进行搜索和访问敏感词的行为。

图表 5-42

5.4.4 上网管理

上网管理功能可以设置上网规则。

图表 5-43

单击 上网规则，进入上网规则页面。

图表 5-44

上网规则包括规则设置、网址白名单、联网程序黑名单。

图表 5-45

5.4.5 安全日志

安全日志包含杀毒日志和事件日志。

5.4.5.1 杀毒日志

杀毒日志可记录 60 天扫描或监控到的病毒日志，可以在隔离区恢复操作。

图表 5-46

5.4.5.2 事件日志

事件日志记录 60 天防护、升级等常见日志，可选择查询指定事件。

图表 5-47

5.5 安全终端 Linux 杀毒

安全终端 Linux 杀毒提供有代理部署场景下的 Linux 系统安全防护功能，不但支持使用客户端设置执行本地查杀，而且能够接收管理中心下发策略进行远程扫描，处理结果以日志形式统一上报管理中心。

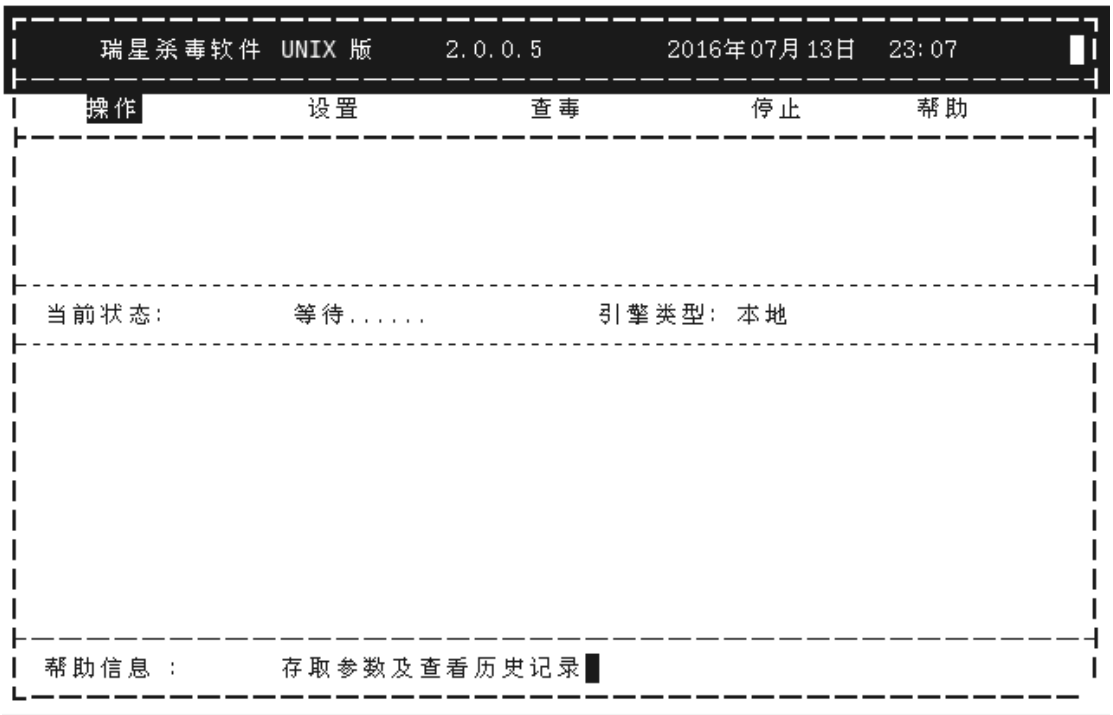
5.5.1 本地查杀

5.5.1.1 字符界面

5.5.1.1.1 菜单说明

从图中可看出，安全终端 Linux 杀毒软件界面的主要功能模块有：操作、设置、查毒、停止和帮助。

查杀毒主界面是使用瑞星杀毒软件 Linux 本地操作的主界面，在此界面上提供了所有的控制选项。



图表 5-48

主菜单栏：用于进行菜单操作的窗口，包括【操作】、【设置】、【查毒】、【停止】、【帮助】五个菜单选项，包括了安全终端 Linux 杀毒本地操作界面提供的所有功能。

染毒文件栏：如果发现病毒，则将感染病毒的文件名、路径、病毒名显示在此窗口中。

无毒文件栏：在此状态栏中显示了当前查杀中无毒文件的路径和文件名。

5.5.1.1.1.1 【查毒】菜单

选择此菜单，即开始扫描病毒。查杀完成后会弹出提示框，显示本次查杀结果，包括总文件、染毒文件、清除文件、删除文件、忽略文件、失败文件。

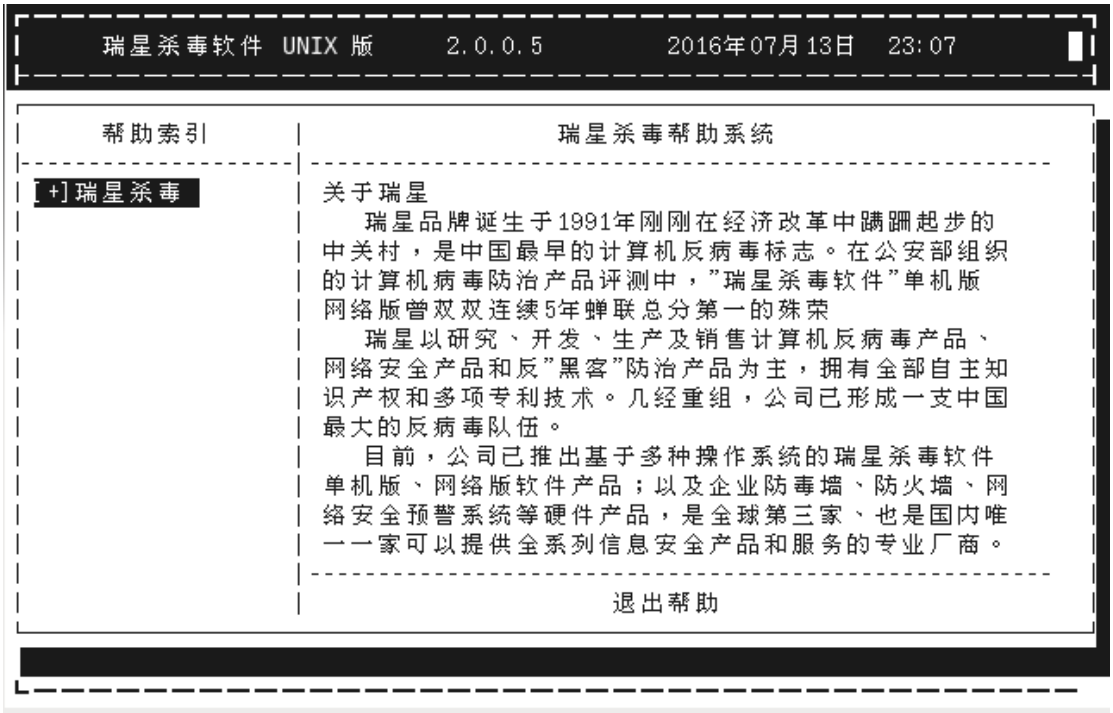
图表 5-49

5.5.1.1.1.2 【停止】菜单

选择此菜单，即停止当前查杀病毒操作。

5.5.1.1.1.3 【帮助】菜单

安全终端 Linux 杀毒提供了常用操作的在线帮助。详细的使用和操作问题请参考本手册，如有其它问题请与瑞星公司客户服务中心联系。



图表 5-50

5.5.1.1.2 查杀病毒

在设置完毕查杀参数后，按 Esc 键退回上级菜单，选择主菜单中的【查毒】或者【杀毒】然后回车，程序即开始按照设置好的参数进行病毒查杀。

在杀毒过程中，如果清除病毒失败，程序会向用户询问如何处理，处理方式有【忽略该文件】、【删除被感染文件】和【停止】。如果想一直使用某种处理方式，请使用空格键或回车键选中【总是使用该选项】。

图表 5-51

5.5.1.1.3 隔离病毒文件的处理

5.5.1.1.3.1 病毒隔离文件的恢复

在病毒隔离记录中用光标移动到要恢复的文件，用“空格”键选中，然后将光标移到【恢复】上后回车（使用 Tab 键移动光标位置）。

图表 5-52

5.5.1.1.3.2 病毒隔离文件的删除

在病毒隔离记录中选中要删除的文件，然后将光标移到【删除】上后回车。

图表 5-53

5.5.1.2 图形界面

5.5.1.2.1 菜单说明

瑞星虚拟化安全终端 Linux 杀毒主程序界面是您使用的主要操作界面，此界面为您提供了瑞星杀毒软件所有的控制选项。通过简单、易操作和友好的操作界面，您无需掌握丰富的专业知识即可轻松的使用瑞星杀毒软件。

图表 5-54

主程序界面包括：

- 菜单栏：用于进行菜单操作的窗口，包括【操作】、【设置】和【帮助】三个菜单选项。
- 查杀目标：主窗体左侧，用于选择需要扫描的目录。
- 病毒列表：主窗体右侧，当扫描发现病毒时，病毒信息（包括文件名、文件路径、病毒名、威胁类型以及状态）将显示在该框中。
- 状态栏：显示了软件的当前版本和更新日期，当扫描或者查杀病毒时，显示文件数、

病毒数和当前扫描文件路径。

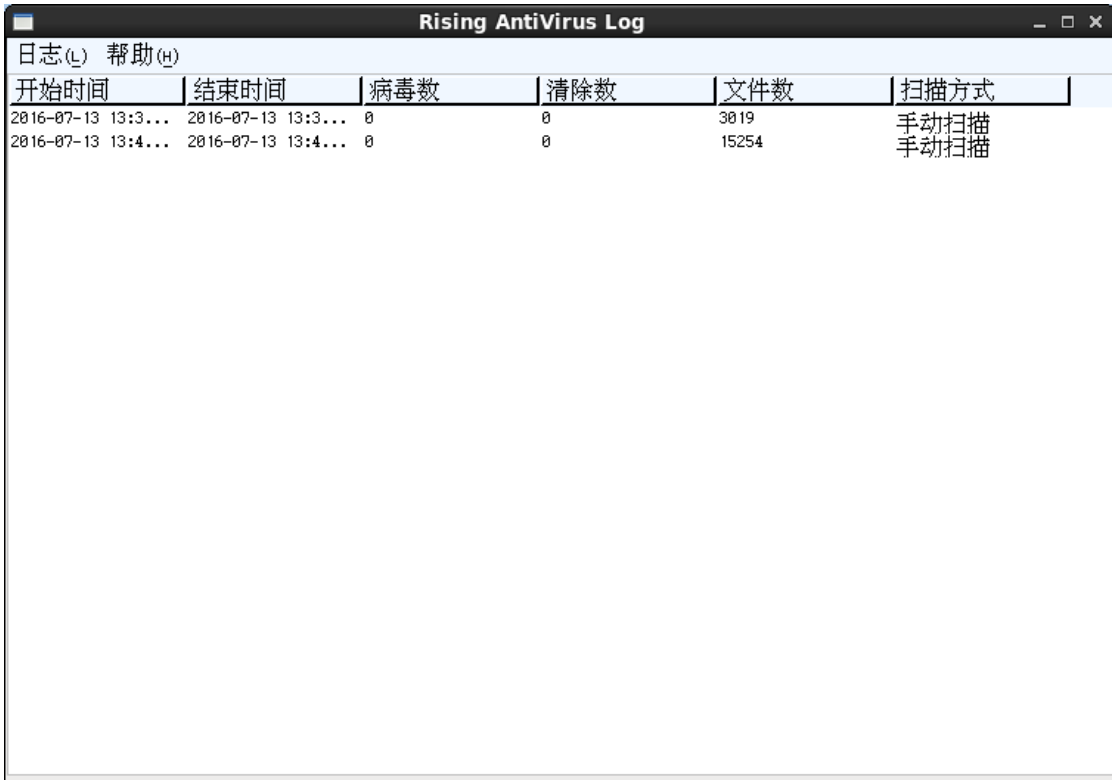
图表 5-55

- 在病毒列表下方，有【杀毒】按钮，查杀病毒时有【暂停】和【停止】按钮。

5.5.1.2.1.1 【操作】菜单

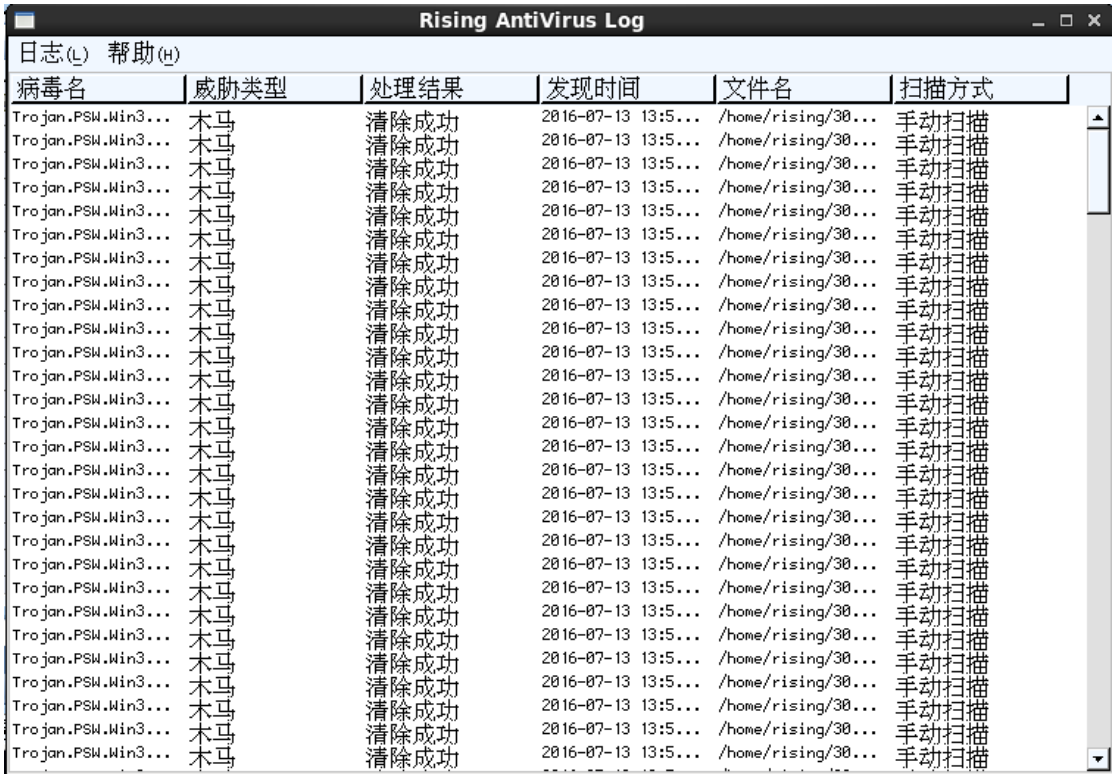
图表 5-56

- 杀毒：对当前查杀目标进行杀毒。
- 停止：结束本次查杀操作。点击停止后，弹出【用户中止】对话框显示查杀结果。
- 病毒隔离系统：启动病毒隔离系统。
- 历史记录：查看扫描日志和病毒日志。
  - 扫描日志：显示所有扫描记录，每条记录内容包括扫描开始和结束时间、病毒数量、清除数量、文件数、扫描方式 。



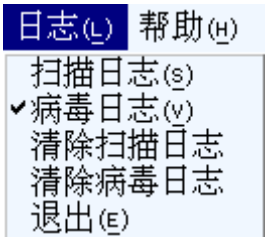
图表 5-57

- 病毒日志：显示所有病毒记录，每条记录内容包括病毒名、威胁类型、处理结果、发现日期、文件名、扫描方式。



图表 5-58

- 清除扫描日志：清除扫描日志列表中的所有扫描日志信息。

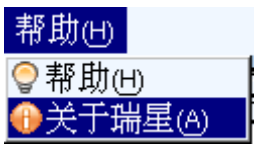


图表 5-59

- 清除病毒日志：清除病毒查杀记录日志信息。
- 退出：退出日志信息界面。

- 退出：退出杀毒软件主程序。

5.5.1.2.1.2 【帮助】菜单



图表 5-60

- 帮助：介绍了软件常用功能，如果在使用瑞星杀毒软件的过程中，用户遇到的疑难问题请联系瑞星客服，客服相关信息请参考附录部分。

关于瑞星：在此可查看瑞星杀毒软件 Linux 图形版的相关信息 。

5.5.1.2.2 查杀病毒

5.5.1.2.2.1 手动查杀

启动瑞星杀毒软件，在主界面左边的“查杀目标”中勾选需要扫描的目录，默认状态下不选择任何目录。

单击【杀毒】按钮或选择【操作】/【杀毒】，开始扫描相应的目录；扫描过程中可随时点击【暂停】按钮来暂时停止扫描，点击【继续】按钮则继续扫描，或点击【停止】按钮停止扫描。

图表 5-61

扫描中，带毒文件名、文件路径、病毒名称和处理状态将显示在查毒结果栏内。

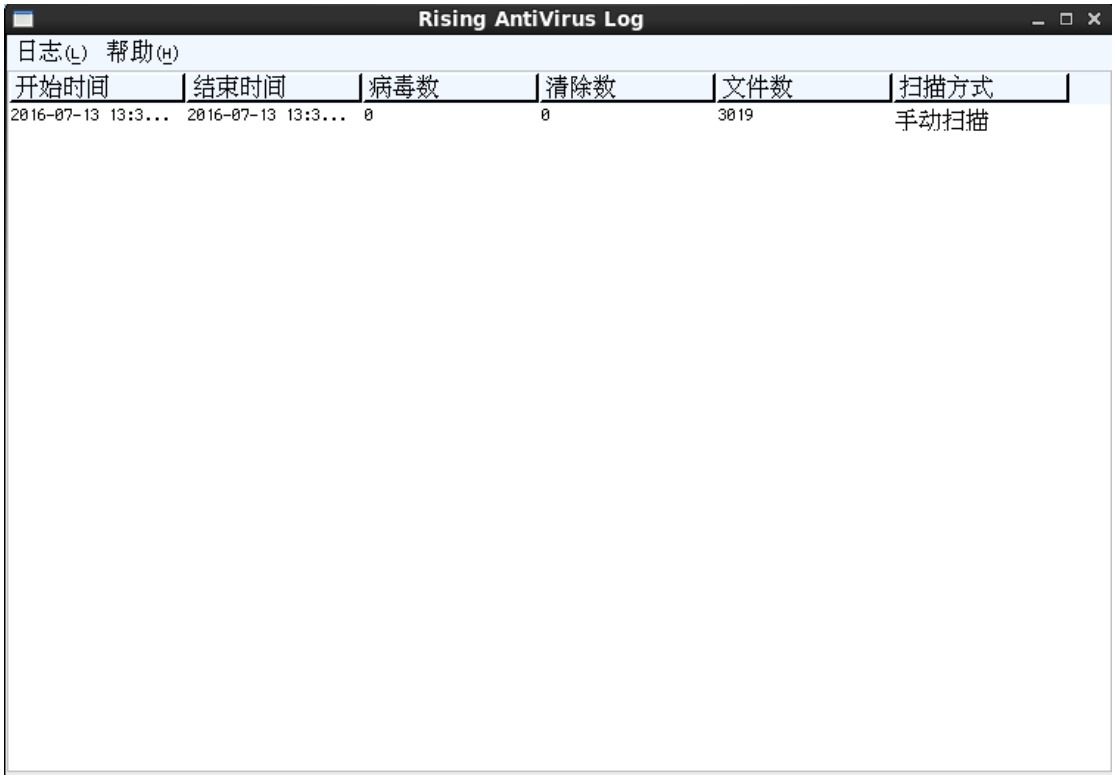
扫描结束后，扫描结果将自动保存到瑞星杀毒软件安装路径下的日志目录中，您可以通过历史记录来查看以往的扫描结果。

5.5.1.2.2.2 查杀记录

为方便用户查看扫描病毒的历史记录，瑞星杀毒软件提供了日志报告。通过日志报告，用户可查看本机扫描病毒的记录，包括开始时间、结束时间、病毒数、清除数、文件数和扫描方式信息。

操作方法：

在瑞星杀毒软件主程序界面中，选择【操作】/【历史记录】。

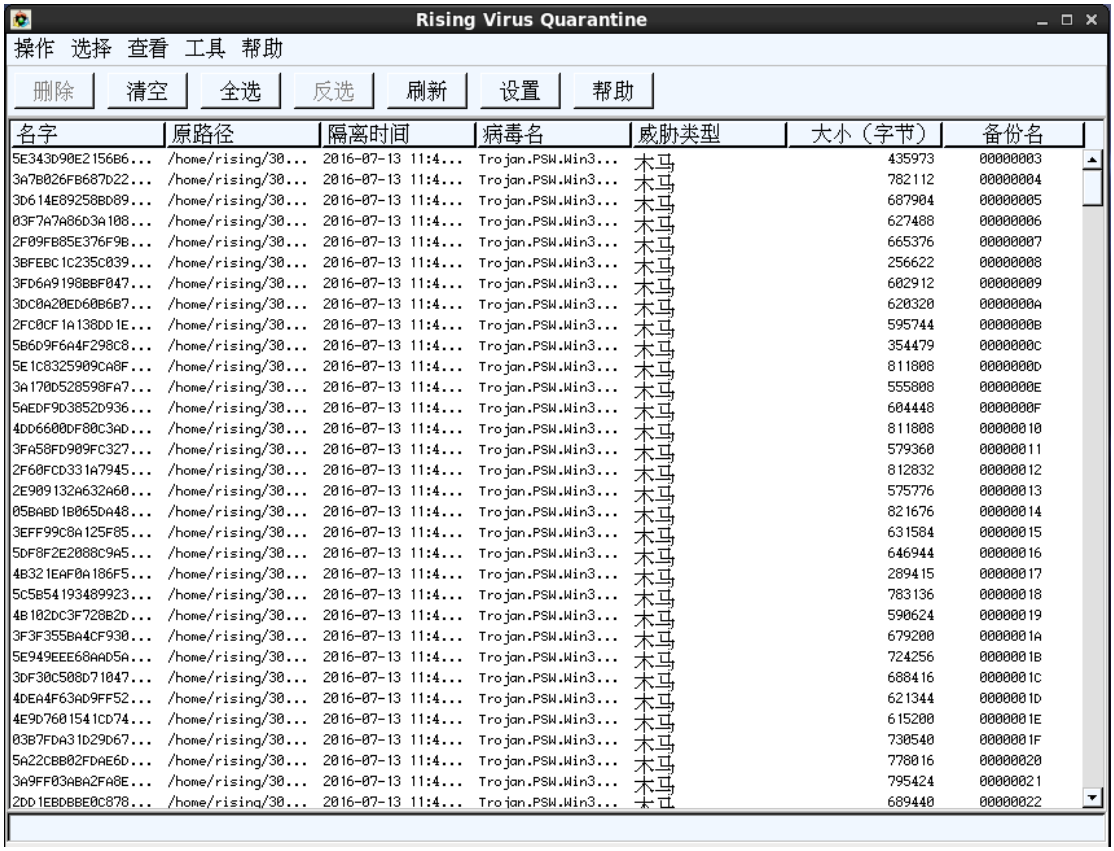


图表 5-62

5.5.1.2.2.3 病毒隔离系统

如果您选择了【将染毒文件备份到病毒隔离系统】（设置方法：在瑞星杀毒软件主程序界面中，选择【设置】/【其它设置】项，在【将染毒文件备份到病毒隔离系统】复选框中勾选），病毒隔离系统将保存染毒文件的备份，保存在病毒隔离系统中的染毒文件不会造成感染破坏。此外，您还可以恢复备份。

在程序的主界面，选择菜单【操作】/【病毒隔离系统】，打开病毒隔离系统设置界面。



图表 5-63

在界面中，最上方为菜单栏，菜单栏下方是快捷操作按钮，中间区域为病毒隔离文件显示栏，最下方为状态栏。

菜单栏：包括操作、选择、查看、工具和帮助；其中，操作可以对隔离文件进行删除、恢复、清空和关闭病毒隔离系统；选择可以对隔离文件进行快速选择，可全部选择、反向选择、相同时间保存的文件、相同路径保存的文件、被相同病毒感染文件。

查看：可以对状态栏、工具栏显示或者隐藏；可以按照时间、位置、路径、大小等方式排列隔离文件顺序。

工具：包括设置隔离区空间。为避免由于备份文件过多而占用大量磁盘空间，病毒隔离系统还可以设置隔离区存储空间。

隔离区大小：默认设置为 500MB，请根据您的实际需求输入设置；

最大文件大小：默认为 20MB，如需隔离更大文件，请重新设置该值；

当隔离空间已满时的处理方式有两种，一是空间自动增长，设置后，隔离区空间大小会根据需要自动增加；二是替换最老文件，设置后隔离区满时将自动删除最老的文件。

图表 5-64

工具栏：包括删除、清空、全选、反选、刷新、设置和帮助。（工具栏如需显示/隐藏，请在查看中设置。）

状态栏：默认显示公司名称，在进行操作时，显示相应操作的输出信息。

5.6Linux 全功能防护客户端

Linux 全功能防护客户端支持使用客户端设置执行本地查杀，而且能够接收管理中心下发策略进行远程扫描，处理结果以日志形式统一上报管理中心。

主要功能包括了 “病毒查杀”、“文件监控”、“网络监控”、“安全工具”和“日志中心”。

5.6.1 病毒查杀

“病毒查杀”是指用户发起的对计算机系统上的磁盘文件进行扫描，并对扫描出的木马病毒进行查杀，该项目包括“自定义查杀”、“快速查杀”、“全盘查杀”等功能模块。

图表 5-65

5.6.1.1 图形界面

5.6.1.1.1 自定义查杀

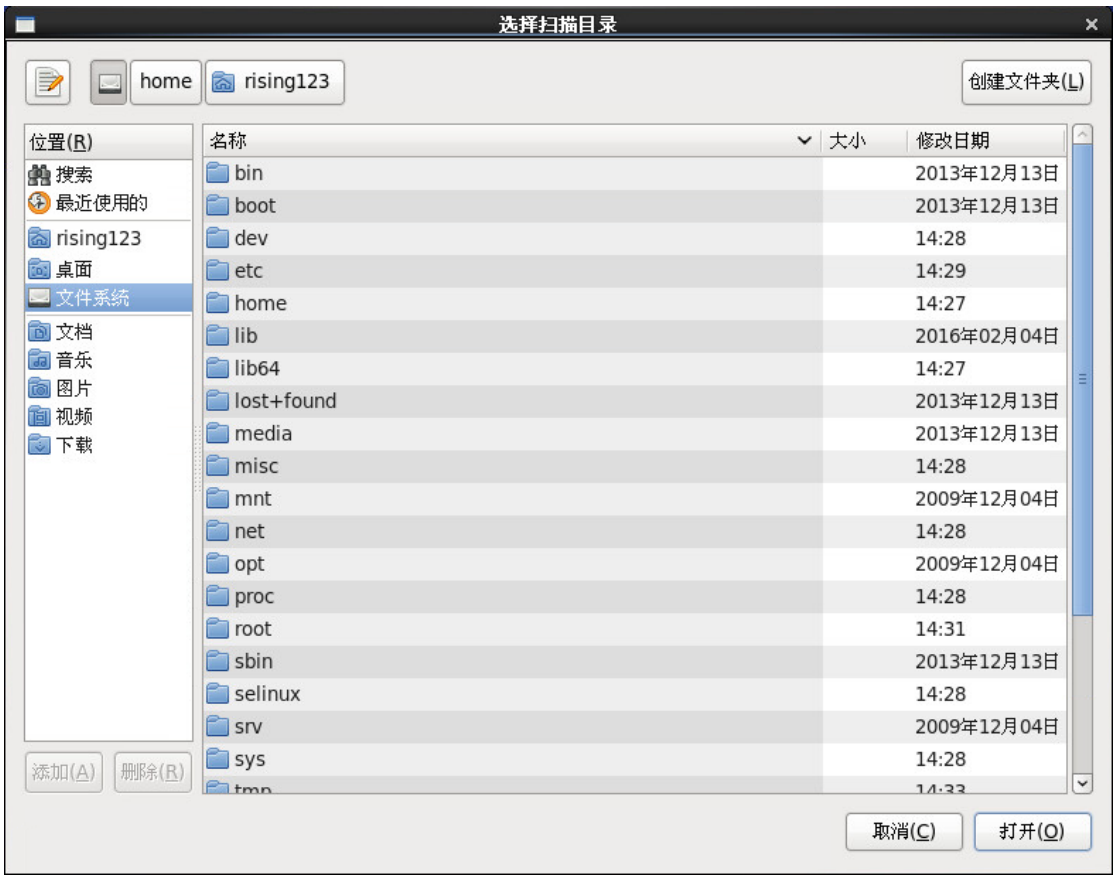
“自定义查杀”可让用户选择一个或多个文件或文件夹进行木马病毒扫描。

查杀某个文件夹下的全部文件：

点击“自定义查杀”。

图表 5-66

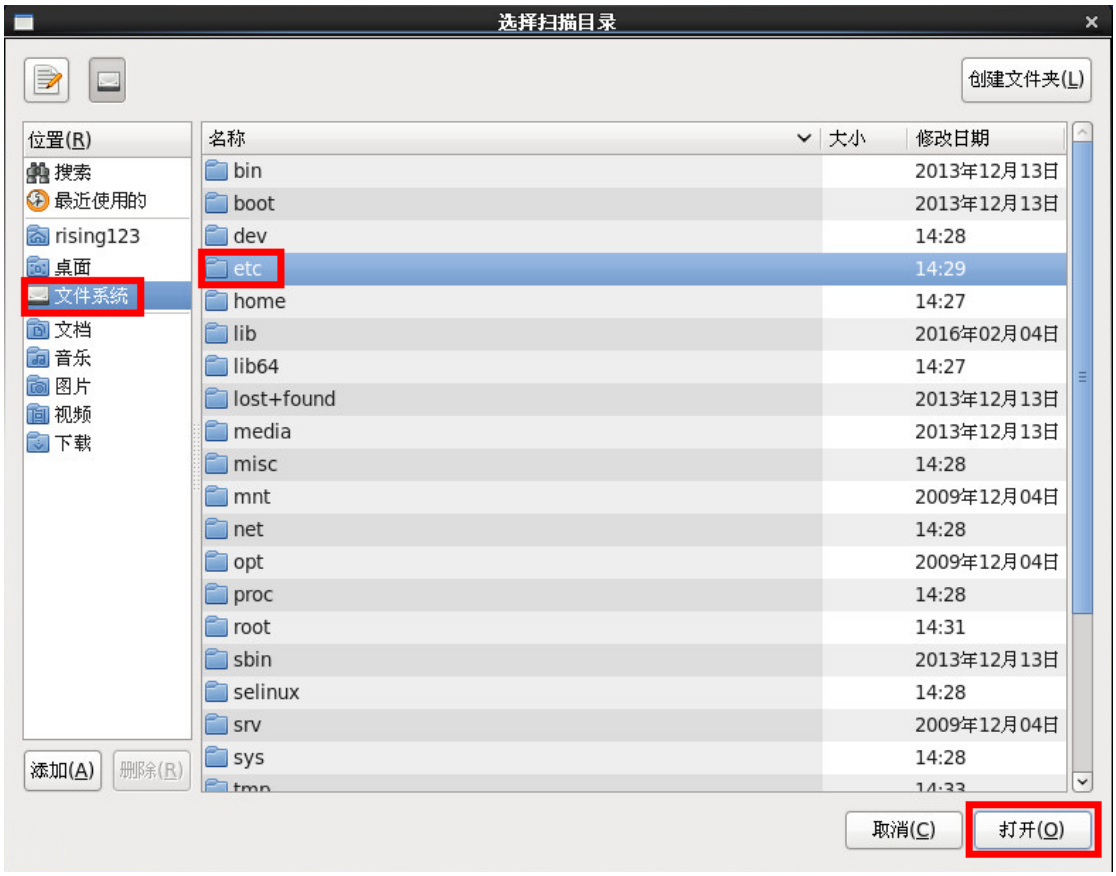
默认打开文件浏览器，展现此计算机系统上的全部文件夹列表，用户可在列表中选择一个文件夹进行扫描。



图表 5-67

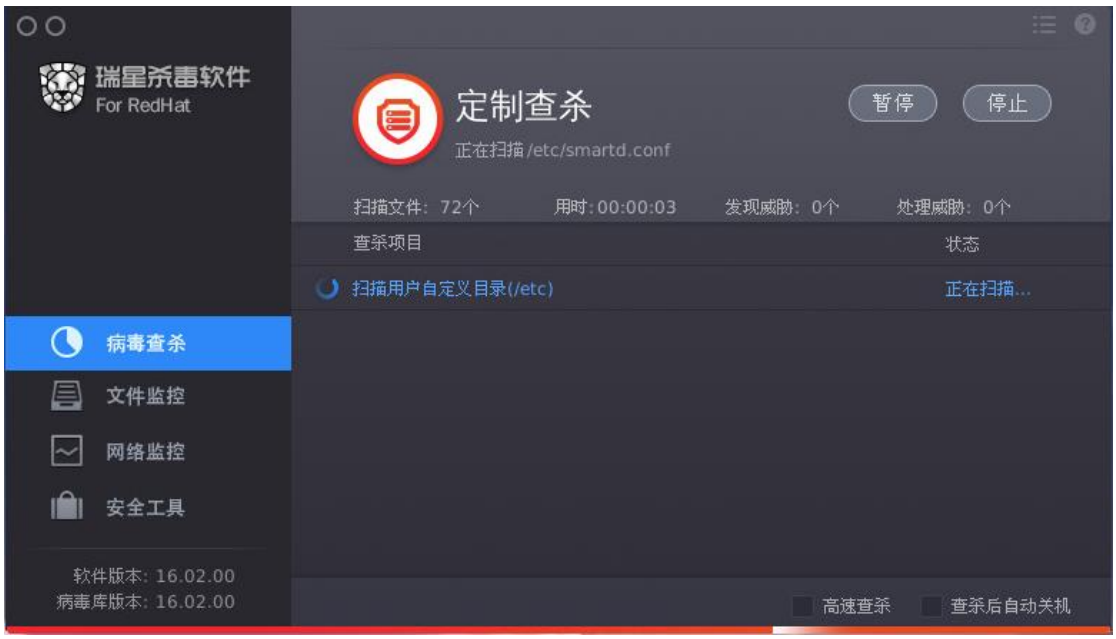
我们在这里选择/etc 文件夹进行扫描，首先在窗口左侧点击“文件系统”，然后在右侧点

击“etc”文件夹，之后点击右下角“打开”开始对此文件夹进行查杀。



图表 5-68

杀毒软件开始对用户指定的目录进行扫描。



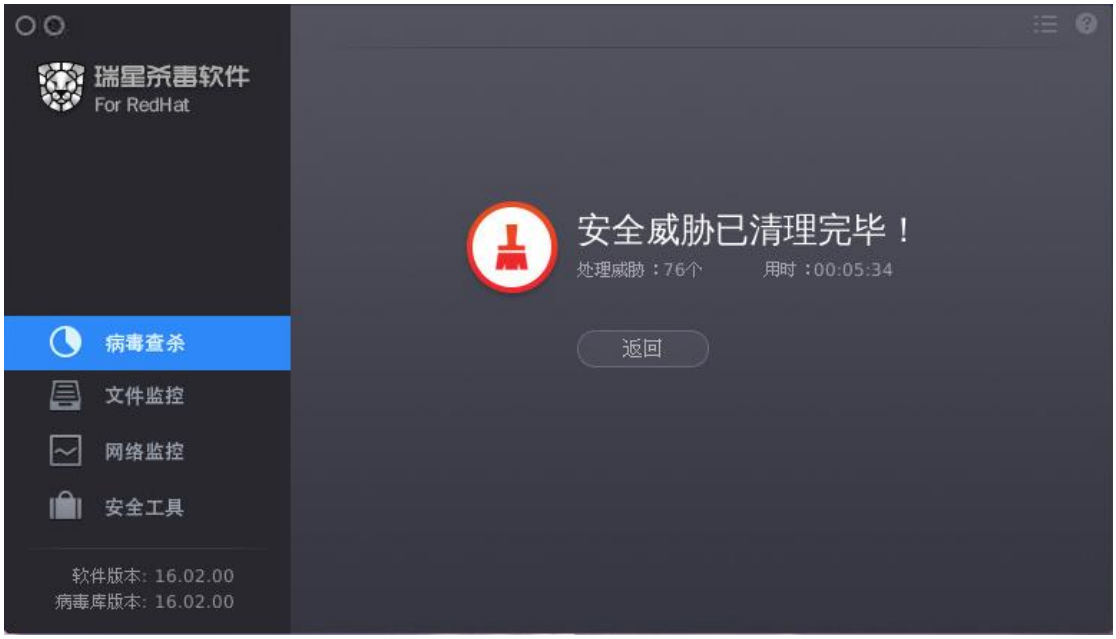
图表 5-69

扫描过程中，软件界面右侧上方实时显示正在扫描的文件，并显示当前一共扫描的文件

数量，所用时间，发现威胁数量（如发现木马病毒等），和处理威胁数量等信息。

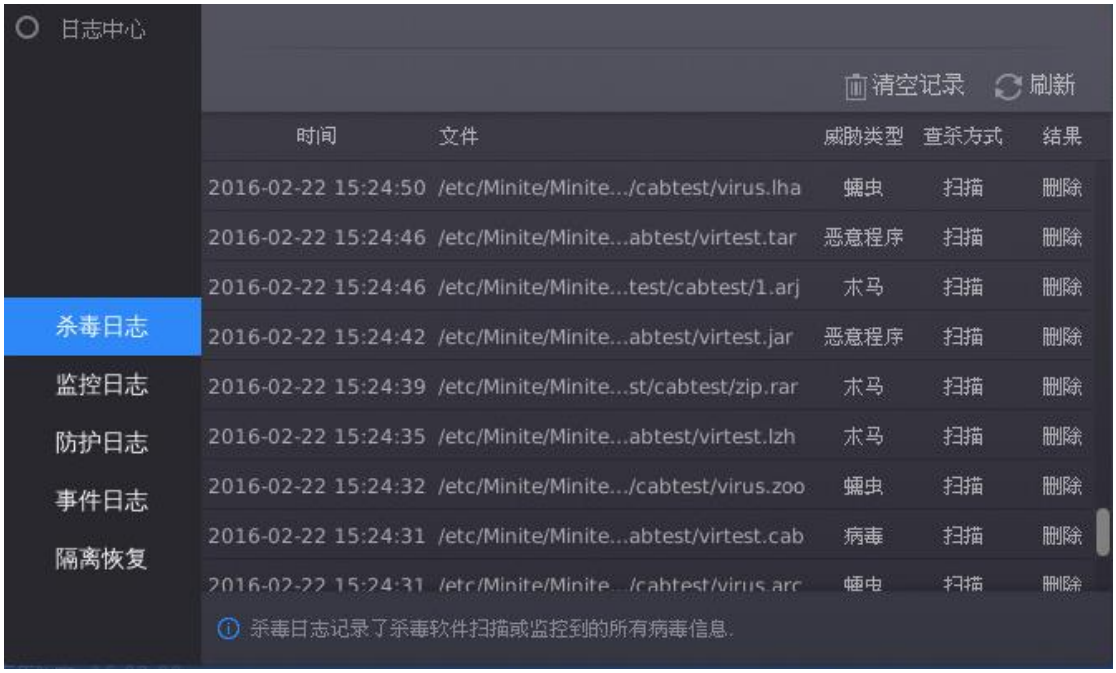
图表 5-70

当扫描结束后，会显示扫描结果，并统计扫描时间。如果发现了木马病毒等威胁，会报告发现并处理的木马病毒数量。



图表 5-71

如果在扫描过程中发现并处理了木马病毒等风险程序，用户可在“日志中心”的“杀毒日志”中看到所查杀病毒木马的具体信息，且“查杀方式”为扫描。



图表 5-72

5.6.1.1.2 快速查杀

“快速查杀”是对系统中的敏感区域和木马病毒常见文件夹进行扫描，它包括了对绝大多数威胁的扫描和检查，同时又比全盘扫描所需的时间更少，是适合大多数用户日常进行扫描的方式。

在“病毒查杀”界面点击“快速查杀”，系统将自动开始对系统敏感区域等位置进行扫描。

图表 5-73

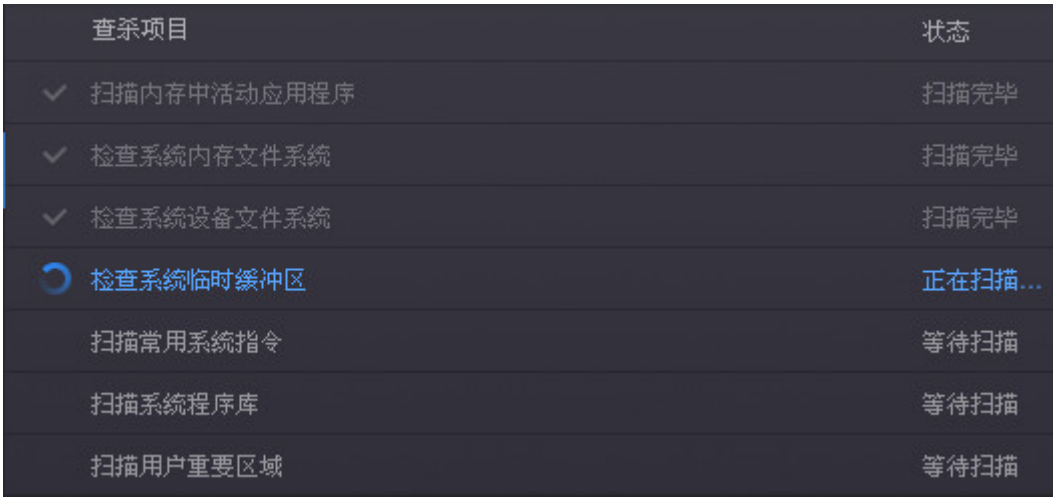
扫描项目具体包括“扫描内存中活动的应用程序”、“检查系统内存文件系统”、“检查系统设备文件系统”、“检查系统临时缓冲区”、“扫描常用系统指令”、“扫描系统程序库”、“扫描用户重要区域”。

图表 5-74

在扫描过程中软件界面右上方显示正在扫描的文件，已经扫描的文件数量，扫描用时，发现威胁和处理威胁的个数。

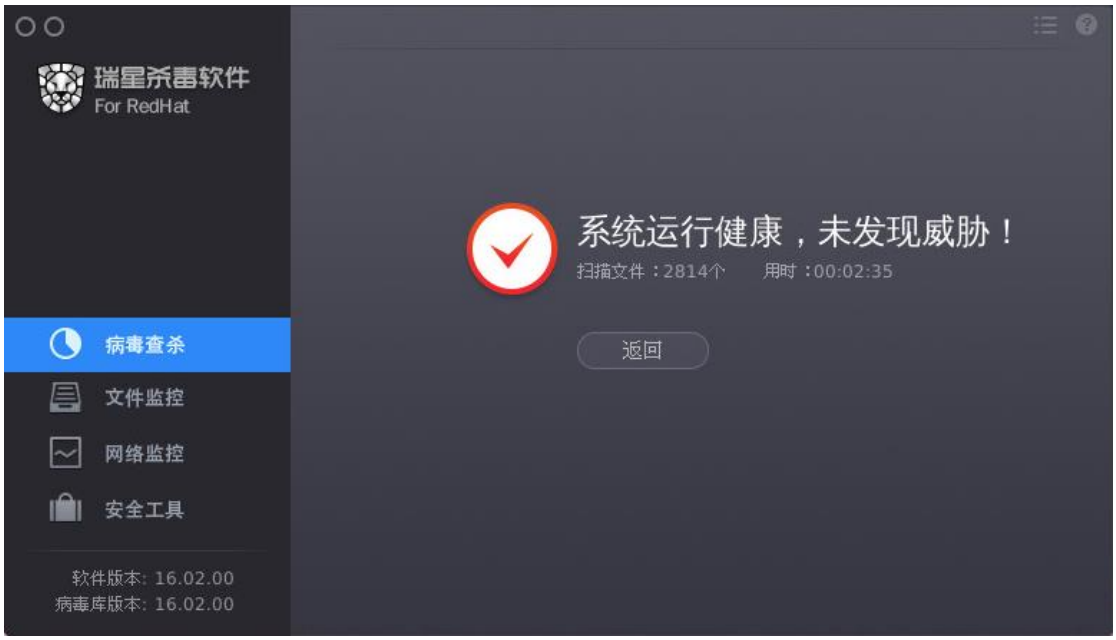
图表 5-75

下方各扫描项目形成列表，扫描自上至下依次进行，其中蓝色字体的项目为当前正在扫描的项目。



图表 5-76

在扫描结束后，界面将展现扫描结果，统计扫描时间，以及发现并处理的威胁程序数量。



图表 5-77

如果在扫描中发现并处理了木马病毒，用户可从“日志中心”的“杀毒日志”中获得详情。

5.6.1.1.3 全盘查杀

“全盘查杀”是指扫描计算机磁盘上的所有文件，根据用户当前磁盘上文件的多少，全盘扫描可能需要几分钟至几十分钟甚至更长时间，它是最彻底的扫描方式，可全方位检查磁盘上可能存在的木马病毒等风险程序。

在“病毒查杀”界面点击“全盘查杀”，系统将自动开始对磁盘上的所有文件进行扫描。

图表 5-78

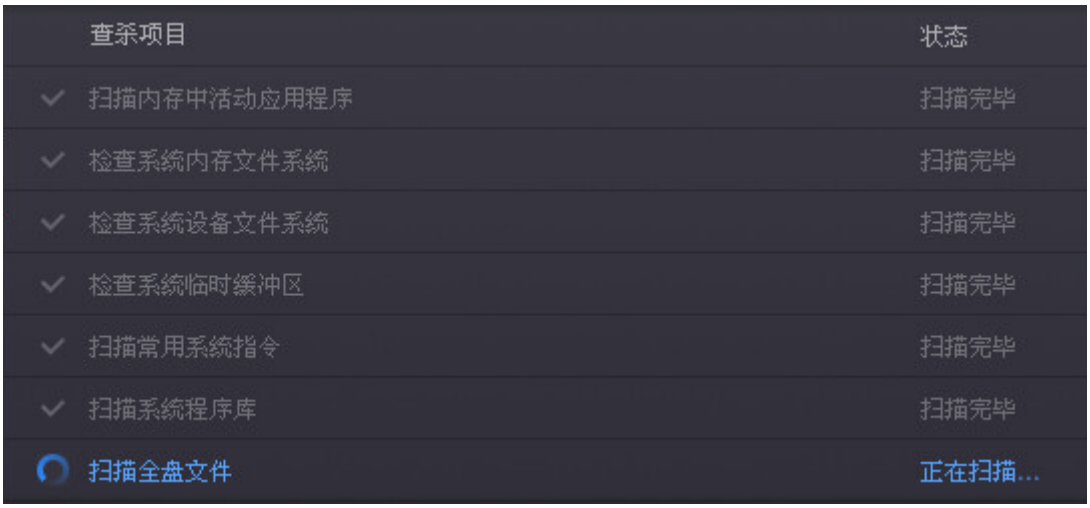
扫描项目具体包括“扫描内存中活动的应用程序”、“检查系统内存文件系统”、“检查系统设备文件系统”、“检查系统临时缓冲区”、“扫描常用系统指令”、“扫描系统程序库”、“扫描全盘文件”。

图表 5-79

在扫描过程中软件界面右上方显示正在扫描的文件，已经扫描的文件数量，扫描用时，发现威胁和处理威胁的个数。

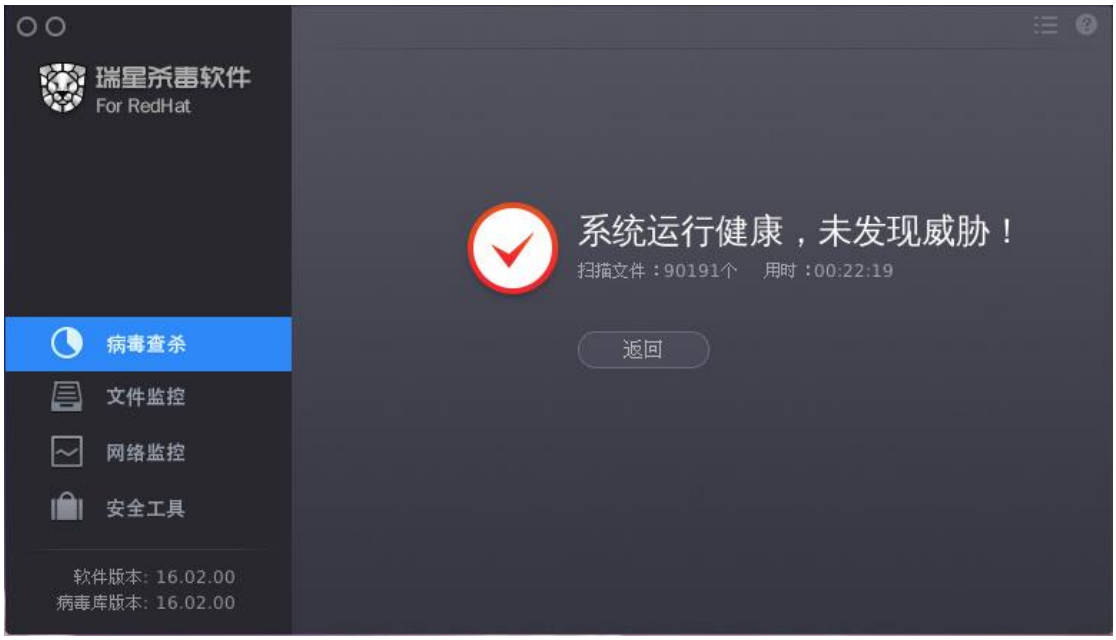
图表 5-80

下方各扫描项目形成列表，扫描自上至下依次进行，其中蓝色字体的项目为当前正在扫描的项目。



图表 5-81

在扫描结束后，界面将展现扫描结果，统计扫描时间，以及发现并处理的威胁程序数量。



图表 5-82

如果在扫描中发现并处理了木马病毒，用户可从“日志中心”的“杀毒日志”中获得详情。

5.6.1.1.4 查杀的暂停、继续及停止

任何一种查杀方式，在其进行过程中都可以将其暂停，继续或停止。

5.6.1.1.4.1 暂停及继续查杀

在查杀进行中，用户可点击界面右侧上方的“暂停”按钮，暂停正在进行的查杀。

图表 5-83

暂停后的查杀任务将进行保持，用户可点击界面右侧上方的“继续”按钮来继续进行此查杀任务。

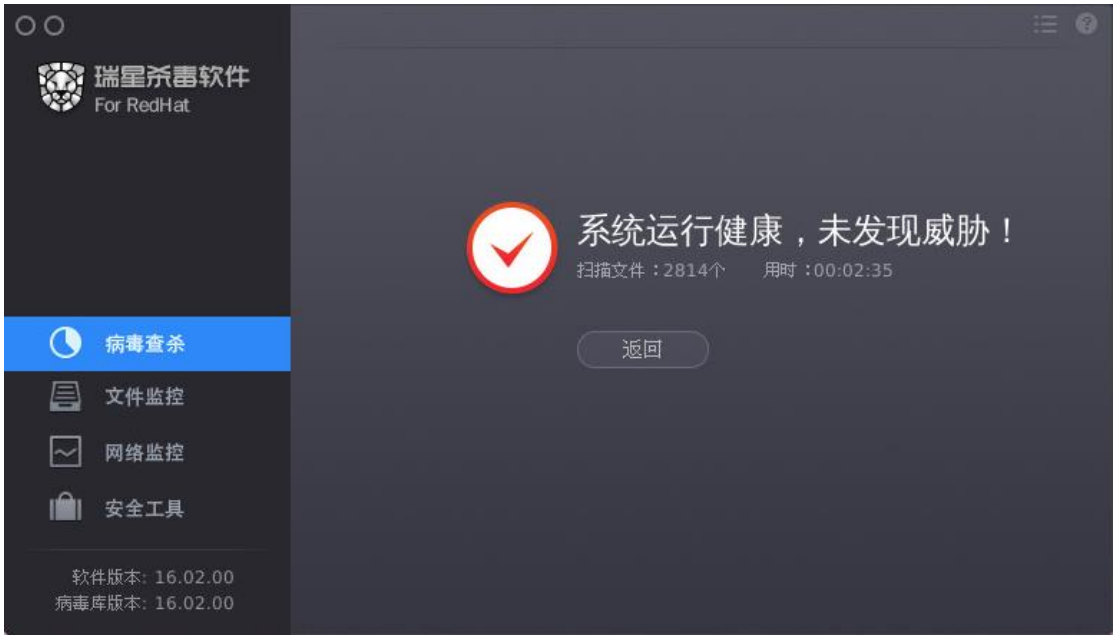
图表 5-84

5.6.1.1.4.2 查杀停止

在查杀进行中，用户可在任何时刻点击界面右侧上方的“停止”按钮来终止本次查杀任务。

图表 5-85

停止后的查杀任务直接结束，显示至停止时扫描的文件个数及所用的扫描时间等信息。



图表 5-86

5.6.1.1.5 高速查杀及查杀后自动关机

5.6.1.1.5.1 高速查杀

在任一查杀任务执行过程中，用户可通过勾选“高速查杀”来加快扫描过程，默认情况下，扫描任务不会占用全部的 CPU 资源，而是根据当前系统的 CPU 占用情况来进行合理的利用，尽量做到在进行扫描任务的同时不影响用户的正常办公及操作，这样，用户不会因为进行扫描任务而感觉到机器明显变慢，但它也限制了扫描的速度，当磁盘中需要扫描的文件很多时，会使扫描过程变得较长，用户可通过勾选查杀界面右下方的“高速扫描”来提高扫描速度，此时杀毒软件将尽可能多的利用 CPU 资源，从而加快查杀速度，但此过程中有可能对用户的其他操作造成一定影响，如电脑执行其他任务反应变慢，请酌情使用。

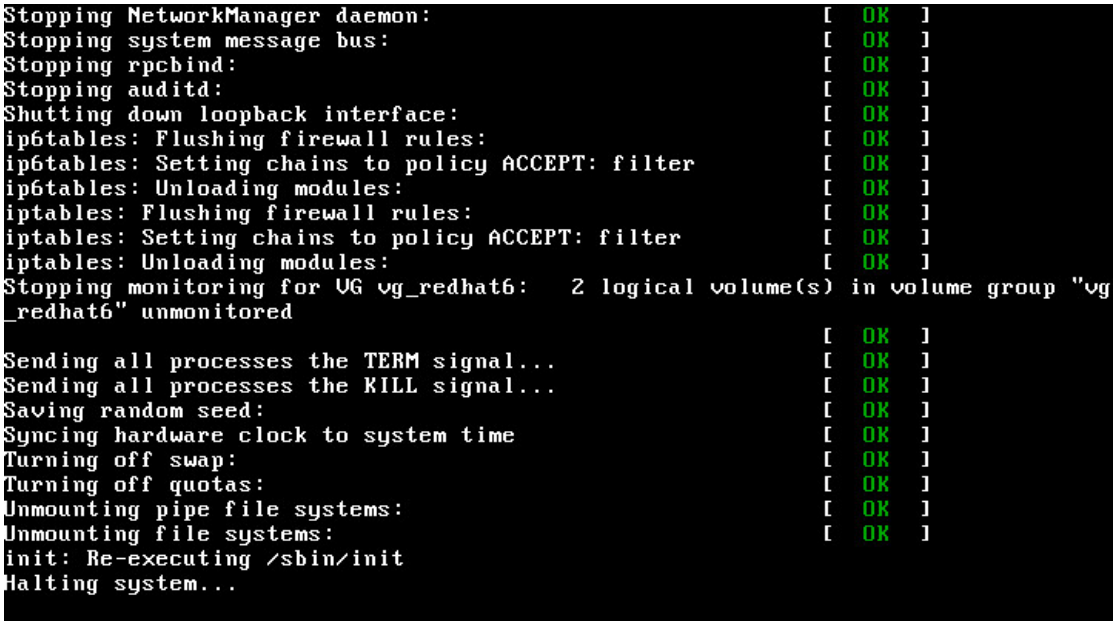
图表 5-87

5.6.1.1.5.2 查杀后自动关机

在查杀任务进行中，用户可勾选软件界面右下方的“查杀后自动关机”选项。

图表 5-88

在查杀结束后计算机将自动关闭。



图表 5-89

5.6.1.2 字符界面

5.6.1.2.1 字符界面下的杀毒软件设置

5.6.1.2.1.1 ravset 命令说明

用户可在字符界面下运行 ravset 命令来进行杀软设置

注意：在字符界面下进行杀软设置不需要root权限，普通用户即可运行。

当用户运行 ravset 命令后，软件在字符界面默认列出此命令所支持的参数及功能说明。

```
[rising123@redhat6 桌面]$ ravset
Usage: ravset [OPTION]

  -a     All current settings are reported
  -c     The item of credible file is adding or deleting. The sub command is 'add' or 'delete'.
          for example:-c 'add /PATH'
  -d     The action when discovering virus
  -f     Only scan file size is less than 20M
  -h     Print this help
  -i     Manager centre's IP
  -o     The os's operation after scaning
  -s     Upload suspicious file when don't confirm scaned file is virus
  -t     Manager centre's port
  -u     Only scan file modified within 15 days
  -v     Print version
```

图表 5-90

ravset 命令的参数和主要设置功能有：

-a All current settings are reported

（-a 列出软件当前所应用的全部设置）

-c The item of credible file is adding or deleting. The sub command is ‘add’ or ‘delete’. for example: -c ‘add /PATH’

（-c 添加或删除可信文件项目，子命令为’add’或’delete’，例如-c ‘add /PATH’ 将添加 /PATH 目录到可信文件项目中）

-d The action when discovering virus

（-d 发现病毒后如何处理，包括隔离、用户选择、或忽略）

-f Only scan file size is less than 20M

（-f 只扫描小于 20M 的文件）

-h Print this help

（-h 打印本命令帮助信息）

-i Manager centre’s IP

（-i 管理平台 PMC 的 IP 地址）

-o The os’s operation after scanning

（-o 完成扫描后的系统操作，包括关机或重启）

-s Upload suspicious file when don’t confirm scanned file is virus

（-s 自动上传发现的可疑文件）

-t Manager centre’s port

（-t 管理平台 PMC 的端口）

-u only scan file modified within 15 days

（-u 只扫描最近 15 天内修改的文件）

-v Print version

（-v 打印软件版本信息，包括软件版本及病毒库版本）

5.6.1.2.1.2 列出当前杀毒软件设置

用户可通过 ravset –a 命令来列出当前杀毒软件所有设置，在用 ravset 命令修改了软件设置后，用户也可通过此命令来确认当前软件的设置信息。

首先用户打开一个终端窗口，运行命令 ravset –a 列出当前杀毒软件的所有设置。

```
[rising123@redhat6 桌面]$ ravset -a
                                linuxRav's settings
---------|----------------------------------------|------------------------------|--------------------|
 command | function                               | default values               | value              |
---------|----------------------------------------|------------------------------|--------------------|
         | protect rav self                       | (yes,no) don't modify        | yes                |
 -s      | upload suspicious file                 | (yes,no)                     | yes                |
 -u      | only scan file modified within 15 days | (yes,no)                     | yes                |
 -f      | only scan file size is less than 20M   | (yes,no)                     | yes                |
 -d      | action when discovering virus          | (quarantine,askme,ignore)    | quarantine         |
 -o      | operation after scaning                | (reboot,shutdown,none)       | reboot             |
 -i      | ipv4 ip address of manager centre      | (255.255.255.255)            |                    |
 -t      | ipv4 port of manager centre            | (0~65535)                    | 0                  |
---------|----------------------------------------|------------------------------|--------------------|
```

图表 5-91

可以看出 ravset 列出了一张表来说明当前系统设置，表的内容包括 command（命令参数）、function（命令功能）、default values（默认值）和 value（设置值）等 4 项内容。

其中第 1 及第 2 列为软件命令参数及其功能说明。

command	function
	protect rav self
-s	upload suspicious file
-u	only scan file modified within 15 days
-f	only scan file size is less than 20M
-d	action when discovering virus
-o	operation after scaning
-i	ipv4 ip address of manager centre
-t	ipv4 port of manager centre

图表 5-92

第 3 及第 4 列为该命令默认值及当前设置值。

default values	value
(yes,no) don't modify	yes
(yes,no)	yes
(yes,no)	yes
(yes,no)	yes
(quarantine,askme,ignore)	quarantine
(reboot,shutdown,none)	reboot
(255.255.255.255)	
(0~65535)	0

图表 5-93

用户在用 ravset 命令修改了软件设置后，可运行命令 ravset –a，并通过最后一列“value（设置值）”来确认软件的设置值。

5.6.1.2.1.3 ravset 命令设置实例

用户通过 ravset 可以完成对杀毒软件进行与图形界面上一样的设置，这里我们以设置“管理平台”PMC 的 IP 地址及端口为例说明 ravset 命令的使用。（本例假设“管理平台”PMC 的 IP 地址为 193.168.12.130，端口为 29443）

若要在命令行设置软件的“管理平台”PMC 的 IP 地址及端口，用户可运行命令：

ravset –i 193.168.12.130 –t 29443

```
[rising123@redhat6 桌面]$ ravset -i 193.168.12.130 -t 29443
[rising123@redhat6 桌面]$
```

图表 5-94

之后用户可再次运行 ravset –a 命令，并观察 value（设置值）中所设置的“管理平台”PMC 的地址及端口。

```
[rising123@redhat6 桌面]$ ravset -a
                                linuxRav's settings
---------|----------------------------------------|------------------------------|--------------------
 command | function                               | default values               | value
---------|----------------------------------------|------------------------------|--------------------
         | protect rav self                       | (yes,no) don't modify        | yes
 -s      | upload suspicious file                 | (yes,no)                     | yes
 -u      | only scan file modified within 15 days | (yes,no)                     | yes
 -f      | only scan file size is less than 20M   | (yes,no)                     | yes
 -d      | action when discovering virus          | (quarantine,askme,ignore)    | quarantine
 -o      | operation after scaning                | (reboot,shutdown,none)       | reboot
 -i      | ipv4 ip address of manager centre      | (255.255.255.255)            | 192.168.15.100
 -t      | ipv4 port of manager centre            | (0~65535)                    | 29443
```

图表 5-95

可以看出“管理平台”PMC 的 IP 地址已经被设置成了 192.168.15.100，端口为 29443。这样就完成了在字符界面下下通过 ravset 命令对杀毒软件的“管理平台”PMC 进行设置。

除了设置“管理平台”PMC 外，ravset 命令还包括其它命令参数，在这里不再一一举例，用户可根据其命令行中的提示及默认值等信息使用 ravset 命令对自己需要的设置在字符界面下进行设置。

5.6.1.2.1 字符界面下的文件扫描

用户可在字符界面下通过命令 ravscan 来发起扫描任务。

```
[rising123@redhat6 桌面]$ ravscan
Usage: ravscan [OPTION]
Scan for virus in memory and filesystem.

  -s, --scan  <path>    customized scan
  -q, --quick           quick scan
  -f, --full            full scan
  -h, --help            print this help
```

图表 5-96

ravscan 命令的参数和主要功能为：

-s， --scan <path> customized scan

（-s --scan <路径> 自定义扫描）

-q， --quick quick scan

（-q --quick 快速扫描）

-f --full full scan

（-f --full 全盘扫描）

5.6.1.2.1.1 字符界面下的自定义扫描

用户可用命令 ravscan –s 来在字符界面下发起对某个文件或某个路径的“自定义扫描”，如扫描/usr 目录，用户可执行命令 ravscan –s /usr。

```
[rising123@redhat6 桌面]$ ravscan -s /usr

Customized scan. Scan path: /usr
Scanned number: 11513, Time used: 5s, Threat number: 0, Killed number: 0
Scanning file: /usr/local/rising/linuxRav/bin/ravgui.zip
```

图表 5-97

软件在扫描过程中会显示当前扫描目录、扫描文件数、扫描用时、发现威胁文件数量（木马病毒等），清除木马病毒数量和正在扫描的文件路径及名称。

扫描结束后，软件会显示是否发现木马病毒，并统计本次扫描的全部文件数量及所用时间。

```
Congratulations! Scanning finished and no threat found.
Scanned file number: 67298
Time used: 00:00:32
```

图表 5-98

5.6.1.2.1.2 字符界面下的快速扫描

用户可用命令 ravscan –q 来在字符界面下发起“快速扫描”任务。

```
[rising123@redhat6 home]$ ravscan -q

Quick scan.
(1/7) Scanning active process in memeory...
(2/7) Checking file system in memeory...
(3/7) Checking device file system...
(4/7) Checking system temporary buffer...
(5/7) Scanning common system commands...
(6/7) Scanning system library...
(7/7) Scanning user home...
Scanned number: 2655, Time used: 5s, Threat number: 0, Killed number: 0
Scanning file: /home/Minite/Minitest-800619/Minitest/Minitest/Vothers/BinLaden.EXE
```

图表 5-99

软件在扫描过程中会显示当前扫描目录、扫描文件数、扫描用时、发现威胁文件数量（木马病毒等），清除木马病毒数量，和正在扫描的文件路径及名称。

扫描结束后，软件会显示是否发现木马病毒，并统计本次扫描的全部文件数量及所用时间。

```
Congratulations! Scanning finished and no threat found.
Scanned file number: 2750
Time used: 00:00:52
```

图表 5-100

5.6.1.2.1.3 字符界面下的全盘扫描

用户可用命令 ravscan –f 来在字符界面下发起“全盘扫描”任务。

```
[rising123@redhat6 home]$ ravscan -f

Full scan.
(1/7) Scanning active process in memeory...
(2/7) Checking file system in memeory...
(3/7) Checking device file system...
(4/7) Checking system temporary buffer...
(5/7) Scanning common system commands...
(6/7) Scanning system library...
(7/7) Scanning all files on disk...
Scanned number: 16500, Time used: 11s, Threat number: 0, Killed number: 0
Scanning file: /home/Minite/Minitest-800619/Minitest/Minitest/cabtest/cleanvir.tar.gz
```

图表 5-101

软件在扫描过程中会显示当前扫描目录、扫描文件数、扫描用时、发现威胁文件数量（木马病毒等），清除木马病毒数量，和正在扫描的文件路径及名称。

扫描结束后，软件会显示是否发现木马病毒，并统计本次扫描的全部文件数量及所用时间。

```
Congratulations! Scanning finished and no threat found.
Scanned file number: 89207
Time used: 00:01:34
```

图表 5-102

5.6.1.2.1 字符界面下扫描发现病毒后的处理

在字符界面下进行磁盘扫描，当发现病毒时会根据用户的设置进行处理，处理方式包括：“隔离”、“用户选择”、或“忽略”。

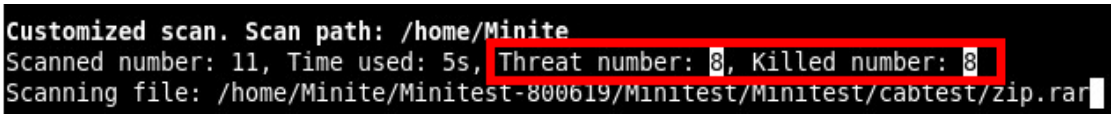
5.6.1.2.1.1 隔离

“隔离”是杀毒软件默认发现病毒的处理方式，在字符界面下用户也可用 ravset –d quarantine 命令来将发现病毒后的处理设置为“隔离”。

```
[rising123@redhat6 home]$ ravset -d quarantine
[rising123@redhat6 home]$
```

图表 5-103

之后软件在扫描过程中发现病毒后会自动对其进行隔离处理。



图表 5-104

在扫描结束后会显示所有威胁文件均被处理，并统计本次扫描的全部文件数量及所用时间。另外还会以红色字体列出威胁文件的详细信息，包括：被感染木马病毒文件的路径及名称、病毒名称，和处理结果。

注意：处理结果为 Killed 代表原被感染文件被清除或删除的同时原文件被放入隔离区。

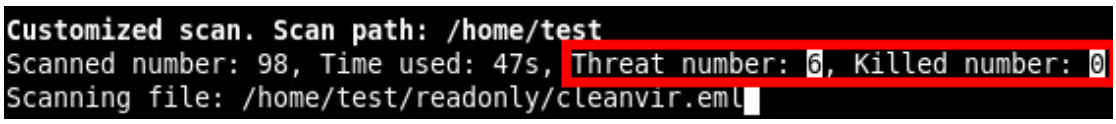
图表 5-105

5.6.1.2.1.2 用户选择

“用户选择”是指当扫描到木马病毒后用户自己决定是否保留这些被感染的文件，在字符界面下用户可用 ravset –d askme 命令来将发现病毒后的处理设置为“用户选择”。

图表 5-106

之后用户在扫描到这些被感染木马病毒的文件后，软件在扫描过程中只会提示扫描出威胁文件数量，但不会对这些文件进行处理。

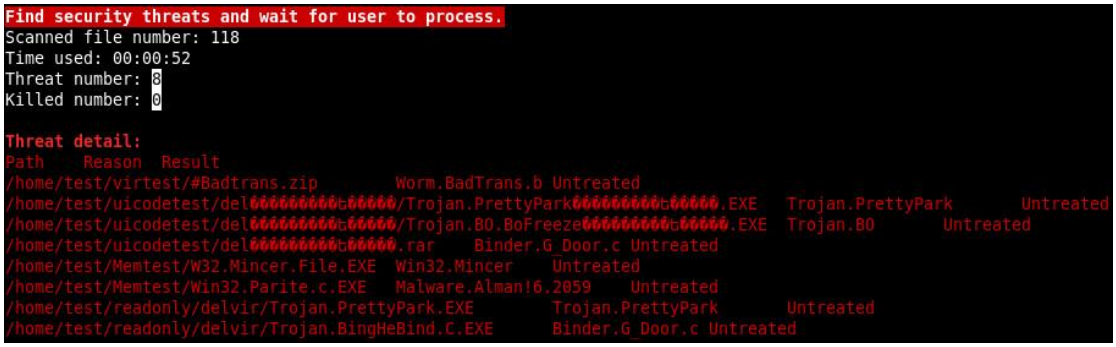


图表 5-107

扫描结束后会显示所有威胁文件均未处理（由用户决定是否保留这些文件），并统计本

次扫描的全部文件数量及所用时间。另外还会以红色字体列出威胁文件的详细信息，包括：被感染木马病毒文件的路径及名称、病毒名称，和处理结果。

注意：处理结果为Untreated代表未处理。



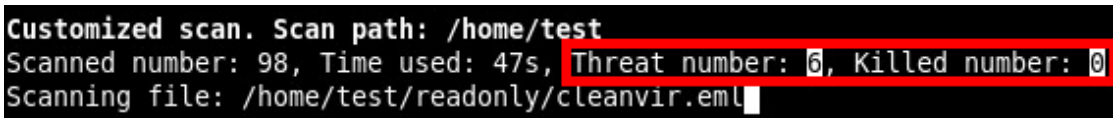
图表 5-108

5.6.1.2.1.3 忽略

“忽略”是指杀毒软件扫描到木马病毒后直接忽略该文件，不进行任何处理。在字符界面下用户可用 ravset –d ignore 命令来将发现病毒后的处理设置为“忽略”。

图表 5-109

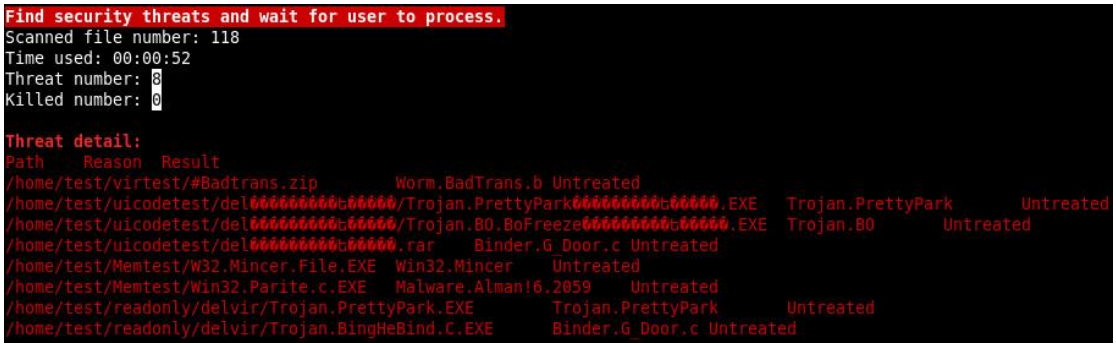
之后用户在扫描到这些被感染木马病毒的文件后，软件在扫描过程中只会提示扫描出威胁文件数量，但不会对这些程序进行处理。



图表 5-110

扫描结束后会显示所有威胁文件均已经被处理（处理方式为“忽略”），并统计本次扫描的全部文件数量及所用时间。另外还会以红色字体列出威胁文件的详细信息，包括：被感染木马病毒文件的路径及名称、病毒名称和处理结果。

注意：此处处理结果为Untreatend代表忽略。



图表 5-111

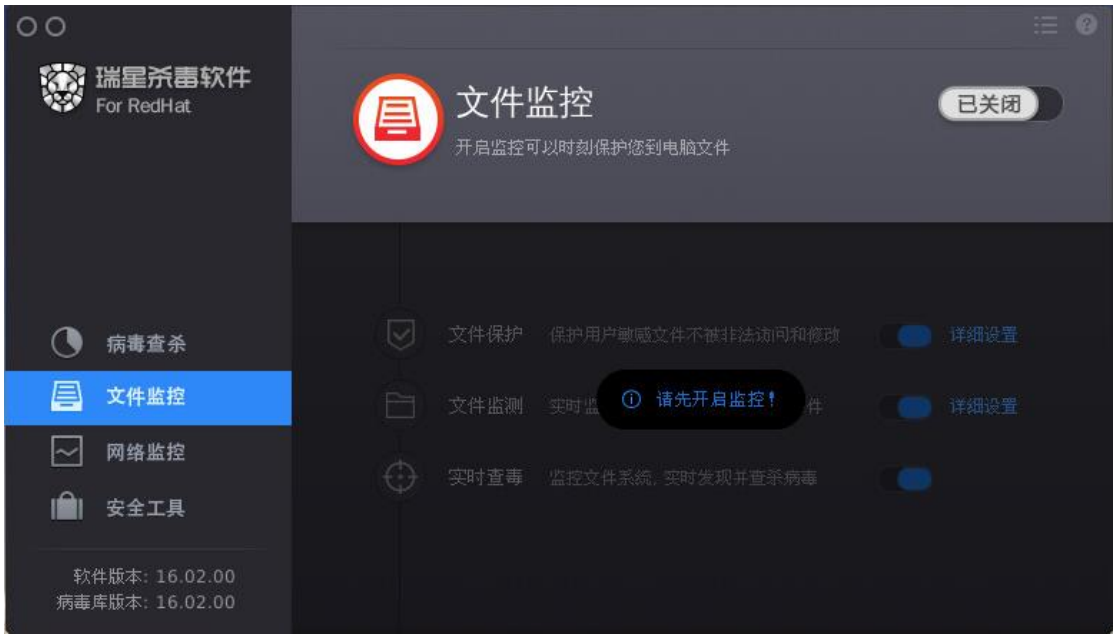
5.6.2 文件监控

文件监控模块实现对系统相关的文件操作进行监控，提供的功能包括：文件保护、文件监测和实时查毒。

注意：文件监控模块的所有功能都需要对瑞星杀毒软件进行授权后才可使用。

5.6.2.1 文件监控的开启及关闭

打开瑞星杀毒软件界面后，在左列选择文件监控，默认文件监控功能关闭。



图表 5-112

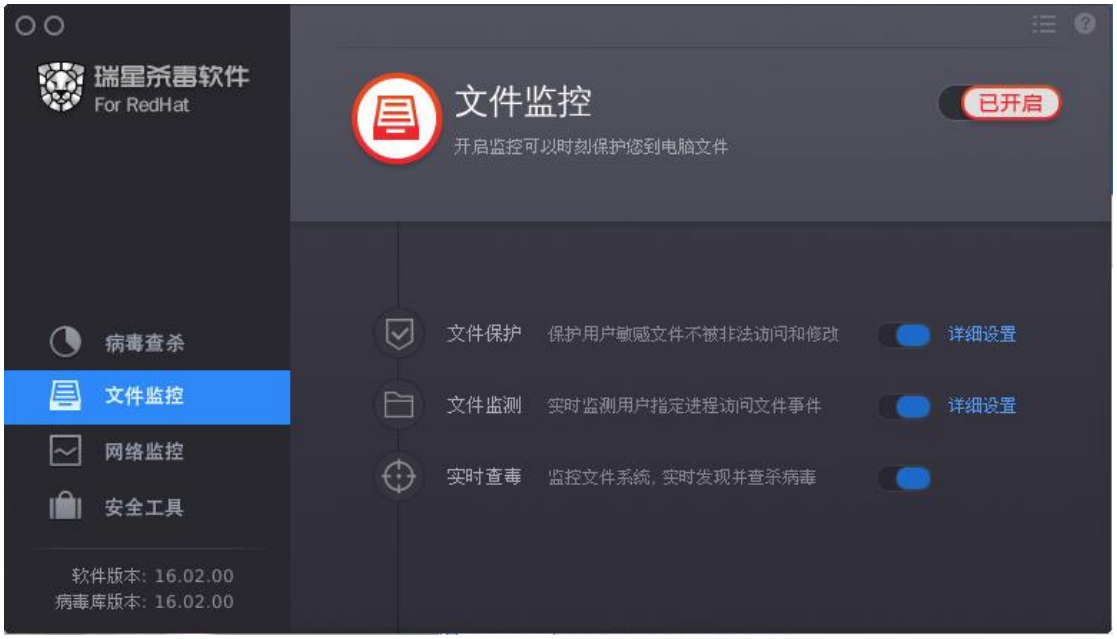
可点击右侧上方“已关闭”开关。

图表 5-113

将其变为“已开启”来打开此功能。

图表 5-114

打开“文件监控”后的软件界面中，默认“文件保护”、“文件监测”及“实时查毒”等功能为开启状态。



图表 5-115

注意，如果提示因授权原因无法开启此功能，请先检查软件是否已经正确分配了授权，在没有正确分配到授权时，此功能无法打开。

图表 5-116

若要关闭“文件监控”功能，可在文件监控“已开启”的状态下，可再次点击该按钮，使其变为“已关闭”来关闭该功能。

5.6.2.2 文件保护

“文件保护”功能可以保护用户敏感文件不被非法访问和修改，用户可在该项目的“详细设置”中添加需要保护的文件，之后根据用户的设置，系统中任何尝试修改或访问该文件的操作都会被告警或阻止，并在日志中有相应的记录。

5.6.2.2.1 文件保护的开启及关闭

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“文件监控”模块其它功能的使用。

首先确认“文件监控”功能已经打开。

图表 5-117

右侧列表中“文件保护”后面的开关为蓝色，说明该功能已经打开。

图表 5-118

若要关闭“文件保护”功能，用户可点击该蓝色开关。

图表 5-119

使其变为灰色时，此功能关闭。

图表 5-120

在“文件保护”功能为关闭状态下，若要再次打开此功能，用户只需再次点击此灰色按钮，使其变为蓝色，则此功能又被打开。

5.6.2.2.2 添加及删除被保护文件

用户可自行添加需要被保护的文件，添加的内容可以是单个文件，又或者是整个目录。

首先确认“文件保护”功能已经开启。

图表 5-121

点击其后方的“详细设置”。

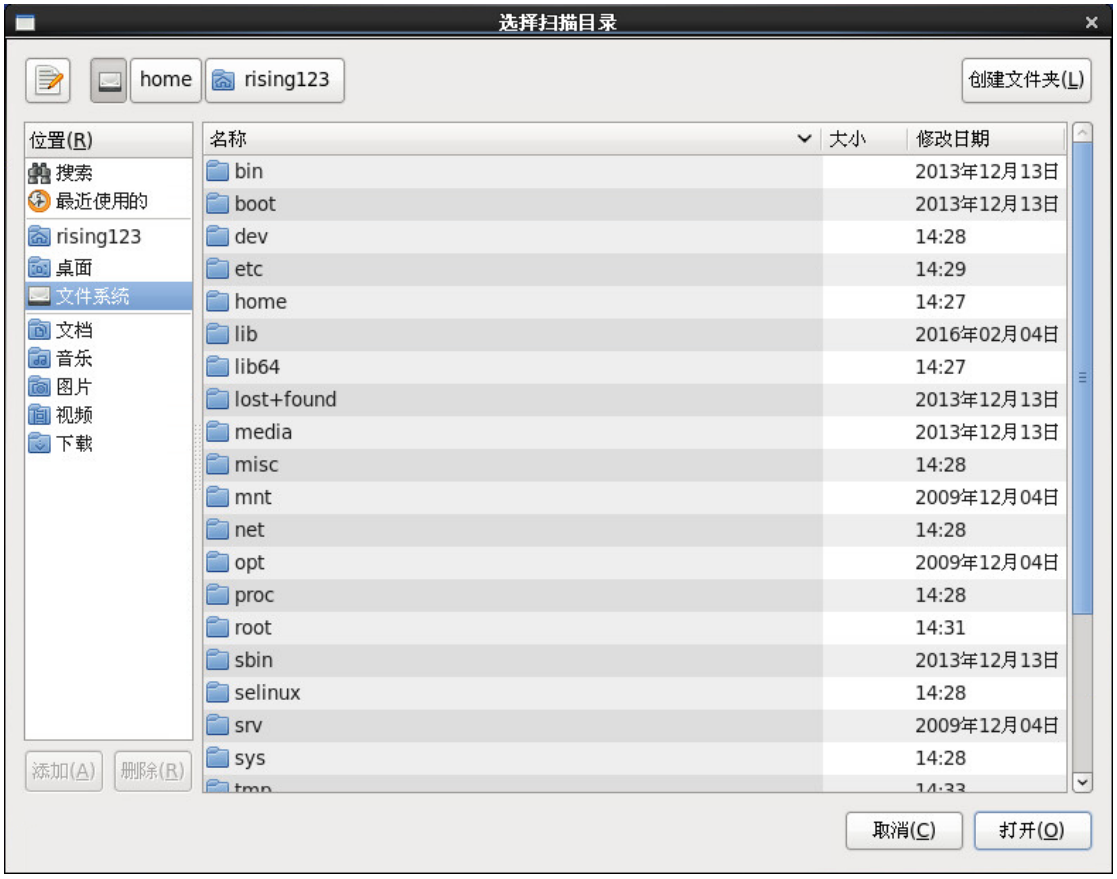
图表 5-122

打开“文件保护”的“详细设置”页面。

图表 5-123

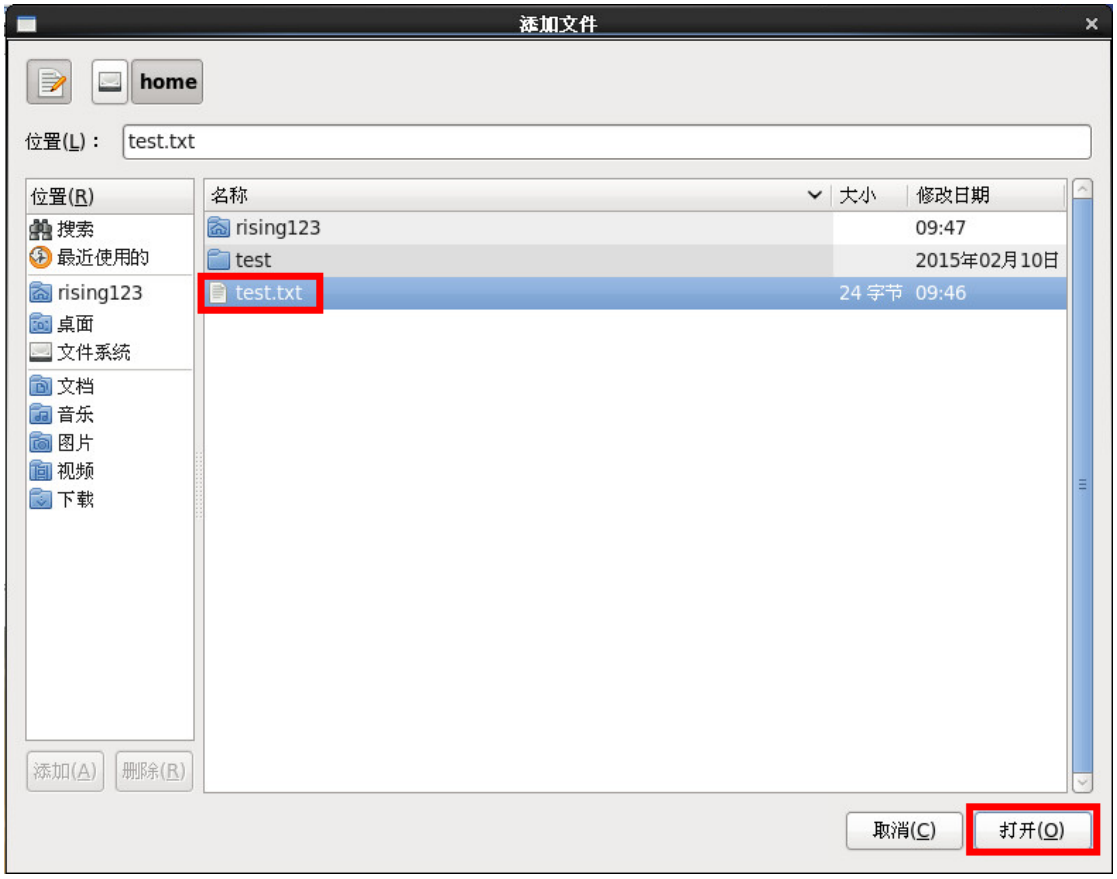
点击右侧上方“添加”按钮，选择“添加文件”，打开文件浏览器。

图表 5-124



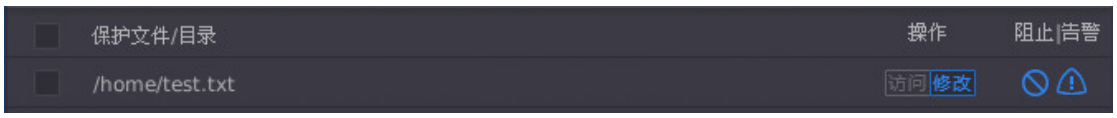
图表 5-125

浏览并选择要被保护的文件，点击右下角的“打开”。



图表 5-126

之后用户可在“文件保护”列表中看到刚刚添加的文件。



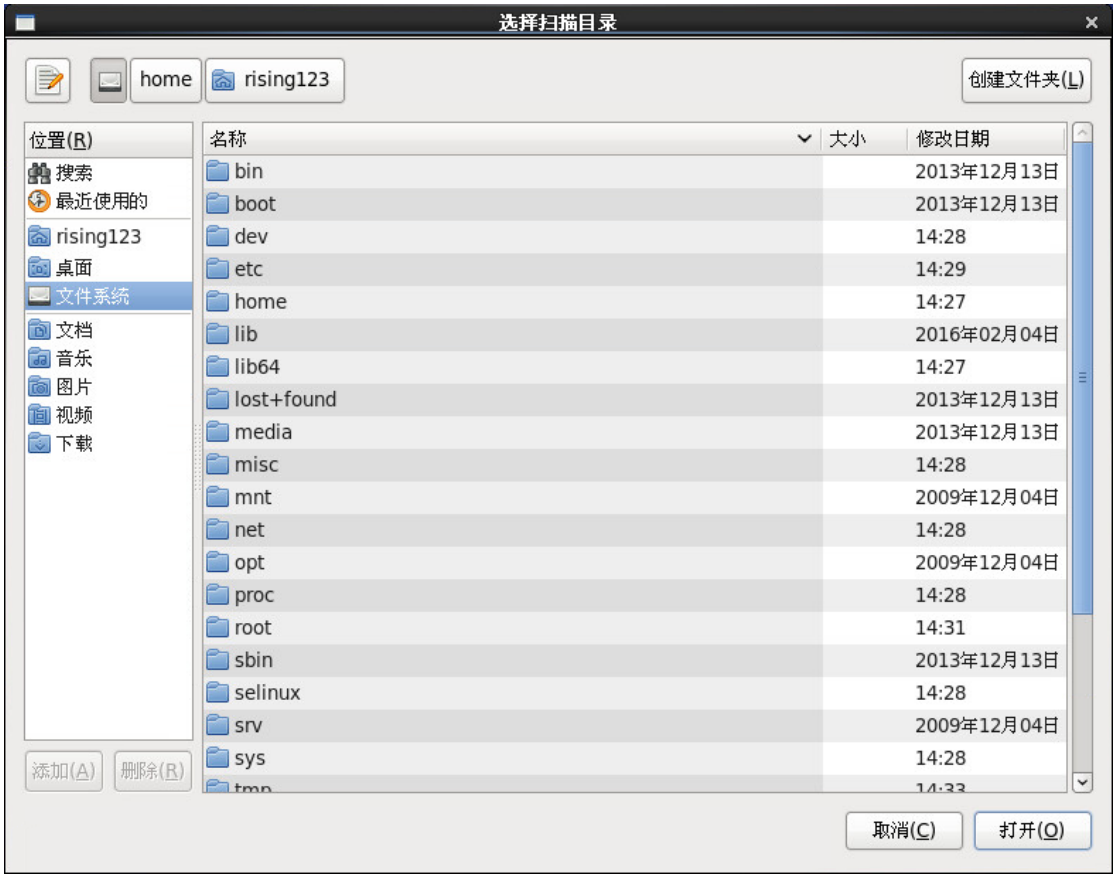
图表 5-127

至此我们就完成了添加单个文件到“文件保护”列表。

除了添加单个文件外，用户还可以添加整个目录到“文件保护”列表以实现对此目录下的所有文件提供“文件保护”功能。

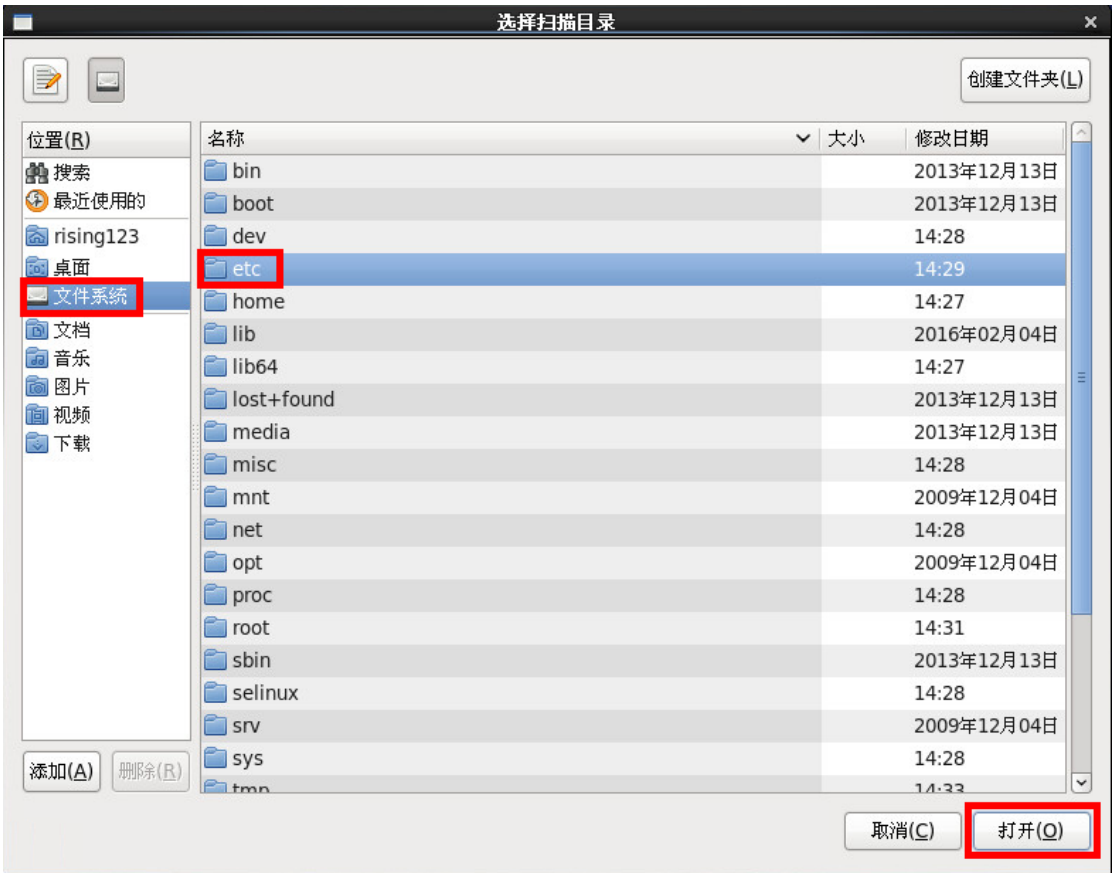
在“文件保护”的“详细设置”页面，点击右侧上方“添加”按钮，选择“添加目录”，打开文件浏览器。

图表 5-128



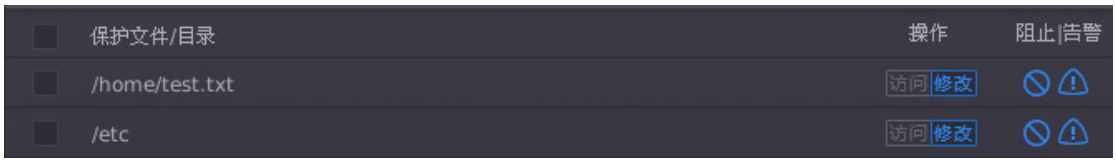
图表 5-129

浏览并选择要被保护的目录，点击右下角“打开”。



图表 5-130

之后用户可在“文件保护”列表中看到刚刚添加的文件目录。

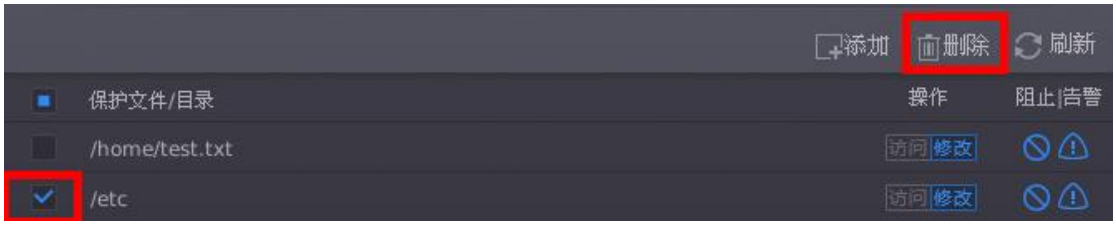


图表 5-131

至此我们就完成了添加某个文件目录到“文件保护”列表。

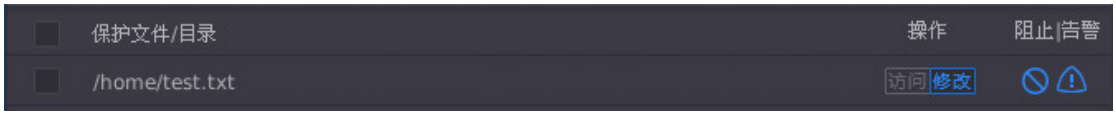
当“文件保护”列表中存在用户所添加的文件或目录时，用户可选择并将其从列表中删除。当列表中存在多个项目时，可以勾选多个项目进行删除。

在“文件保护”列表中，勾选要删除的文件或目录，然后点击右上方的“删除”按钮。



图表 5-132

之后，列表中被删除的项目消失。

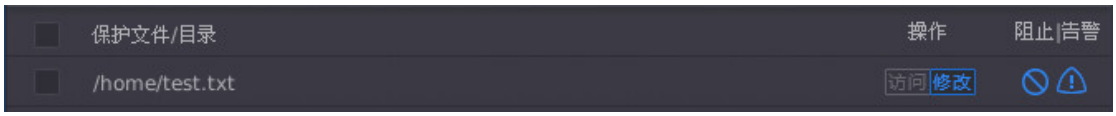


图表 5-133

这样就完成了对“文件保护”列表中项目的删除。

5.6.2.2.3 监控并阻止修改文件

当用户在“文件保护”列表中添加了某文件时，默认设置为监控并阻止对此文件的修改，并记录日志。比如我们在列表中添加一个/home/test.txt，默认该项目“操作”栏的“修改”以及“阻止”“告警”选项都为蓝色（蓝色代表开启状态）。



图表 5-134

注意：当用户在列表中添加了希望被“文件保护”监控到的文件后，需要点击页面左上角的X关闭此页面，才可让设置生效。

图表 5-135

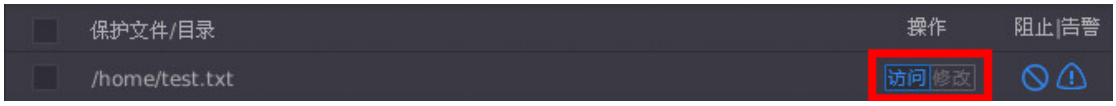
这时如果尝试对此文件进行修改，在保存时将会失败。

图表 5-136

同时在“日志中心”的“防护日志”中会有相应阻止修改的记录。

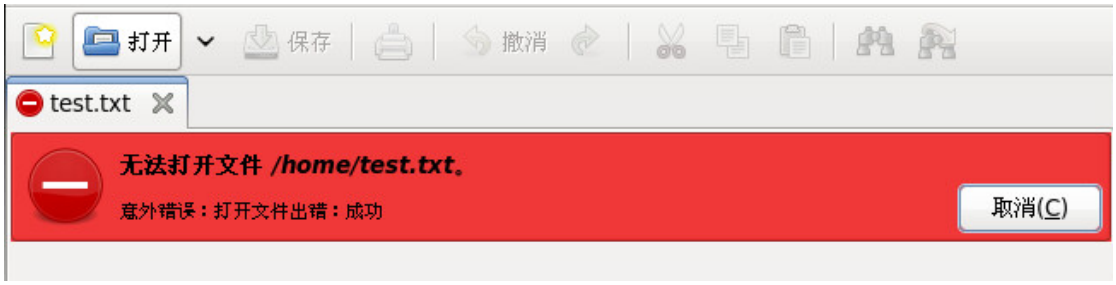
图表 5-137

若用户在“文件保护”列表中点击操作栏的“访问”，此时“访问”为蓝色（同时关闭了监控文件“修改”的功能）。



图表 5-138

此时尝试访问该文件（如尝试用编辑器打开该文件）将会失败。

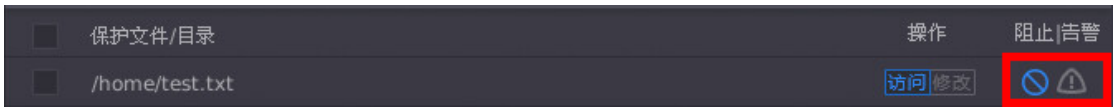


图表 5-139

同时在“日志中心”的“防护日志”中会有相应的阻止读取的记录。

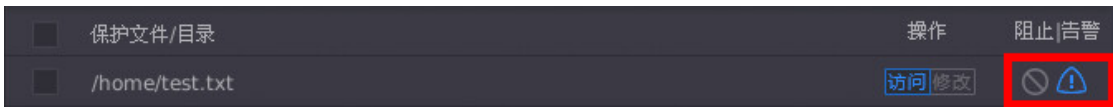
图表 5-140

除了选择“访问”或“修改”外，用户还可选择是否对该文件的操作进行“阻止”或“告警”，当用户保留“阻止”图标为蓝色，点击“告警”图标，使其变为灰色（相当于关闭了告警功能）时，对该文件的“访问”或“修改”将被“阻止”，但不会有日志记录。



图表 5-141

相反，若用户保留“告警”功能，而关闭“阻止”功能，对该文件相应的操作将被允许，但会在“日志中心”的“防护日志”中有相应的允许访问记录。



图表 5-142

图表 5-143

“文件监测”功能可以让用户指定监控某个可运行的程序或某个正在后台运行的进程，监控其对文件的访问等操作，并记录相关的日志。

5.6.2.2.4 文件监测的开启及关闭

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“文件监控”模块其它功能的使用。

首先确认“文件监控”功能已经打开。

图表 5-144

之后观察右侧列表中“文件监测”后面的按钮为蓝色，说明该功能已经打开。

图表 5-145

若要关闭“文件监测”功能，用户可点击该蓝色按钮，使其变为灰色时，此功能关闭。

图表 5-146

图表 5-147

在“文件监测”功能为关闭状态下，若要再次打开此功能，用户只需再次点击此灰色按钮，使其变为蓝色，则此功能又被打开。

5.6.2.2.5 添加或删除监控的进程或可执行程序

用户可自行添加需要被监测的可执行程序，添加的内容可以是某个正在运行的进程，又或者是某个可执行程序。

注意：添加不可执行的程序将没有监测效果。

首先确认“文件监测”功能已经开启。

图表 5-148

点击其后方的“详细设置”，打开“文件监测”的详细设置页面。

图表 5-149

图表 5-150

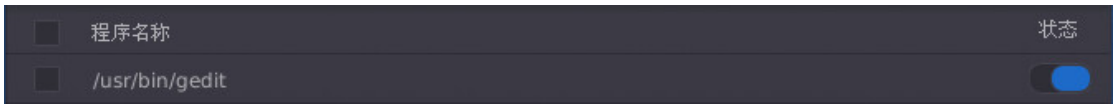
点击右侧上方“添加”按钮，选择“添加进程”（这里我们假设文本编辑程序 gedit 已经在刚才被打开运行，且一直未关闭），在进程窗口里找到并选择 gedit 进程，并点击“确定”。

图表 5-151

图表 5-152

之后用户可在“文件监测”程序列表中看到刚刚被添加的进程，且该进程的“状态”为开启

监测（蓝色开关）。



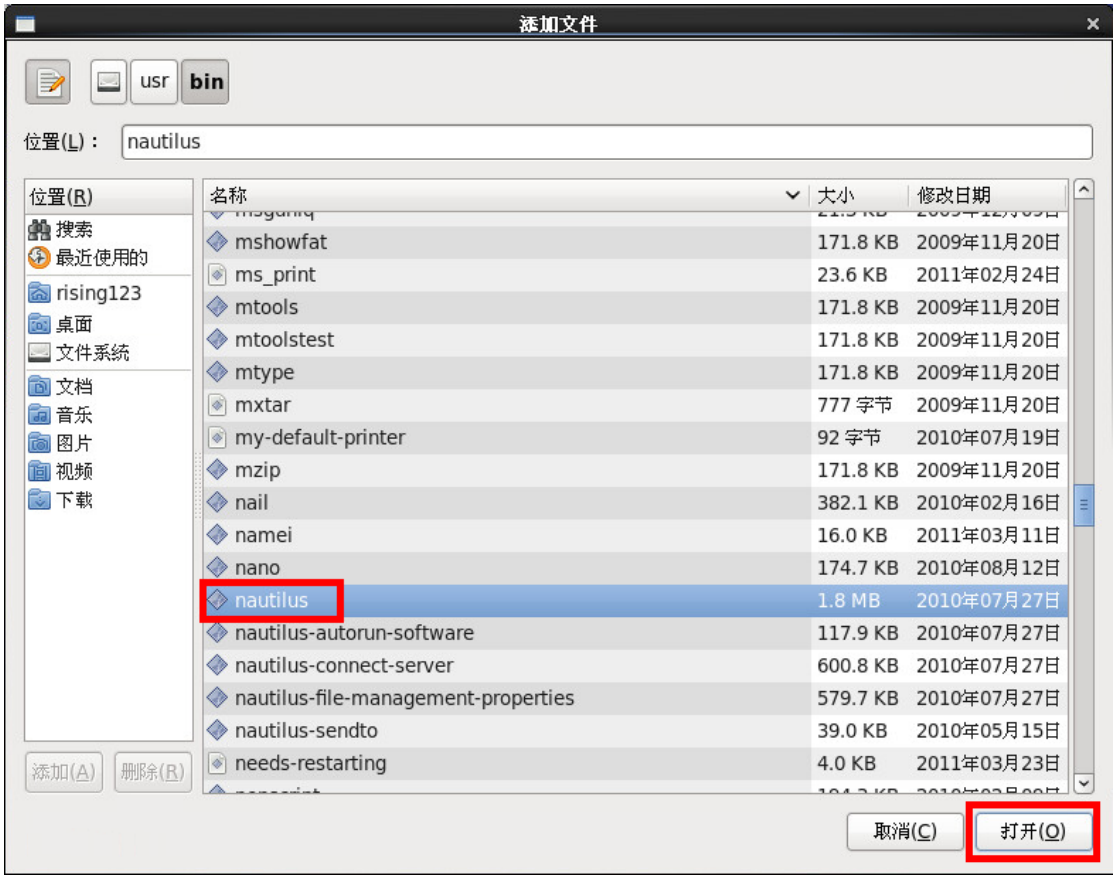
图表 5-153

至此我们就完成了添加某个正在运行的进程到“文件监测”列表当中。

除了添加正在运行的进程，用户还可以添加某个可以被执行的程序到“文件监测“列表中。

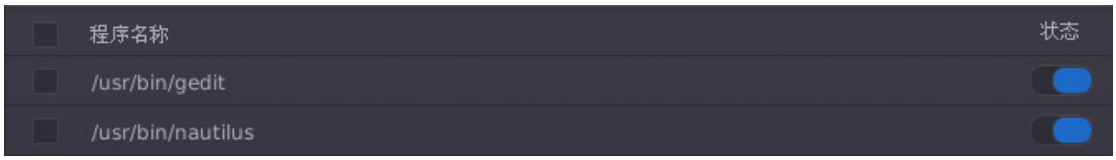
点击右侧上方“添加”按钮，选择“添加文件”，打开文件浏览器，浏览并选择要添加的程序，点击右下角“打开”。

图表 5-154



图表 5-155

之后用户可在“文件监测”程序列表中看到刚刚被添加的程序，且该程序的“状态”为开启监测（蓝色开关）。

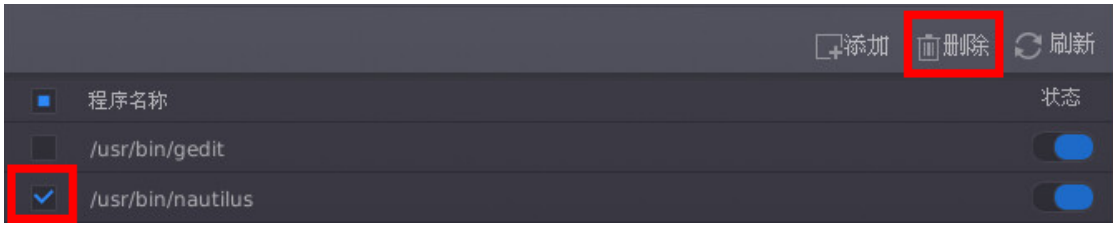


图表 5-156

至此我们就完成了添加某个可以被执行的程序到“文件监测”列表当中。

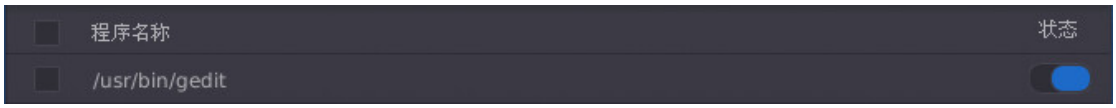
当“文件监测”列表中存在用户所添加的进程或可执行程序时，用户可选择将其从列表中删除。当列表中存在多个项目时，可以勾选多个项目进行删除。

在“文件监测”列表中，勾选要删除的进程或可执行程序，然后点击右上方的“删除”按钮。



图表 5-157

之后，列表中被删除的项目消失。



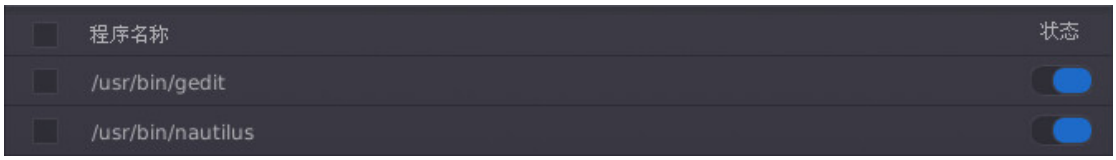
图表 5-158

这样就完成了对“文件监测”列表中项目的删除。

5.6.2.2.6 关闭或打开某个“文件监测”项目

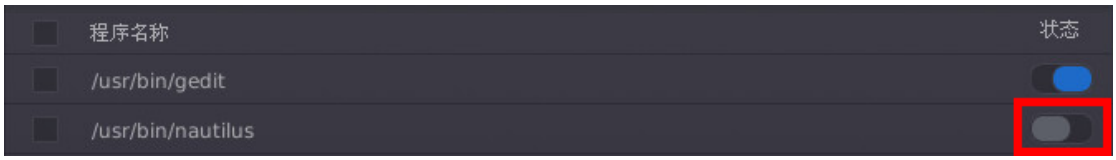
当“文件监测”列表中存在一个或多个进程或可执行程序时，用户可选择是否打开对某个或某几个项目的监测。只有打开监测（开关为蓝色）的项目会被监测。

当进程或程序被添加到“文件监测”列表当中时，其监测状态默认为开启（蓝色开关）。



图表 5-159

用户可点击不希望被监测项目的开关，当其变为灰色时，则对相应项目的监测功能关闭。

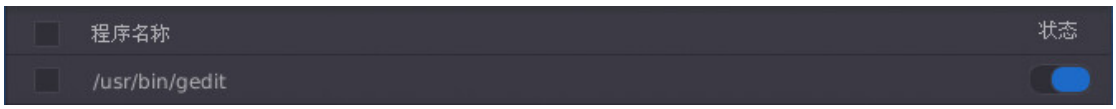


图表 5-160

对于列表中已经被关闭监测的项目，用户可再次点击该开关，当期变为蓝色时，对相应项目的监测功能再次开启。

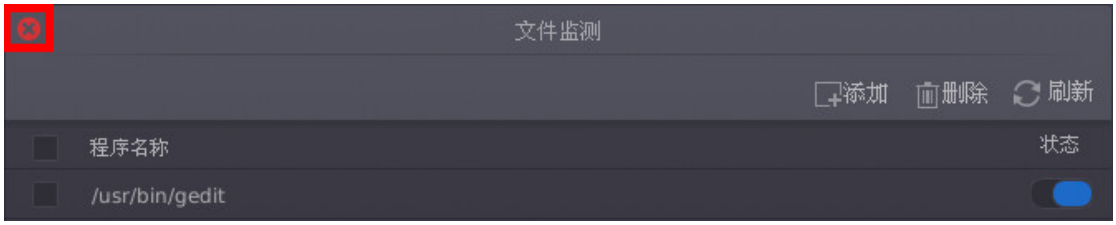
5.6.2.2.7 文件监测功能实例

首先在“文件监测”列表中添加想要被监控的可执行程序，（这里我们以 gedit 为例），并确保其“状态”为开启监测（蓝色开关）。



图表 5-161

注意：当用户在列表中添加了希望被“文件监测”监控到的可执行程序，或修改了其状态开关后，需要点击页面左上角的X关闭此页面，才可让设置生效。

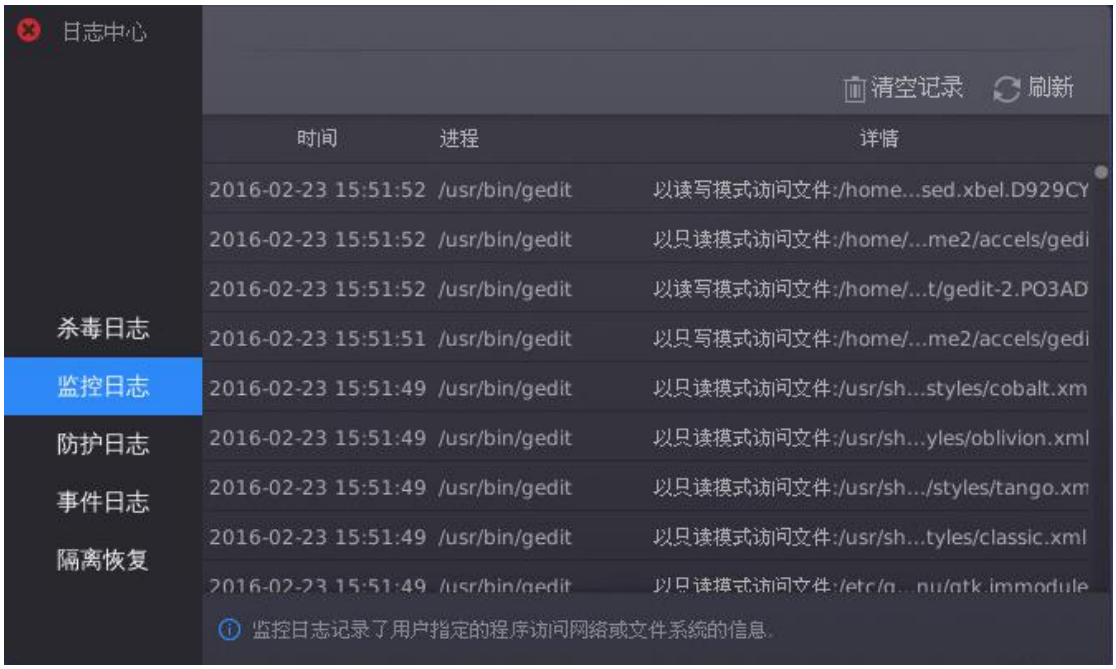


图表 5-162

然后打开 gedit 程序，过一会将其关闭。

图表 5-163

之后到“日志中心”，查看“监控日志”，发现很多 gedit 在运行时所打开各文件的详细记录。



图表 5-164

至此我们就成功监测到了 gedit 程序运行过程中所打开并访问的文件。

5.6.2.3 实时查毒

“实时查毒”提供木马病毒的实时监控功能，可以实时检查到正在进行打开或被复制等操作的文件，如果文件含有木马病毒，将会被实时查杀，并记录相关日志。

5.6.2.3.1 实时查毒的开启及关闭

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“文件监控”模块其它功能的使用。

首先确认“文件监控”功能已经打开。

图表 5-165

之后观察右侧列表中“实时查毒”后面的按钮为蓝色，说明该功能已经打开。

图表 5-166

若要关闭“实时查毒”功能，用户可点击该蓝色开关，使其变为灰色时，此功能关闭。

图表 5-167

图表 5-168

在“实时查毒”功能为关闭状态下，若要再次打开此功能，用户只需再次点击此灰色按钮，使其变为蓝色，则此功能又被打开。

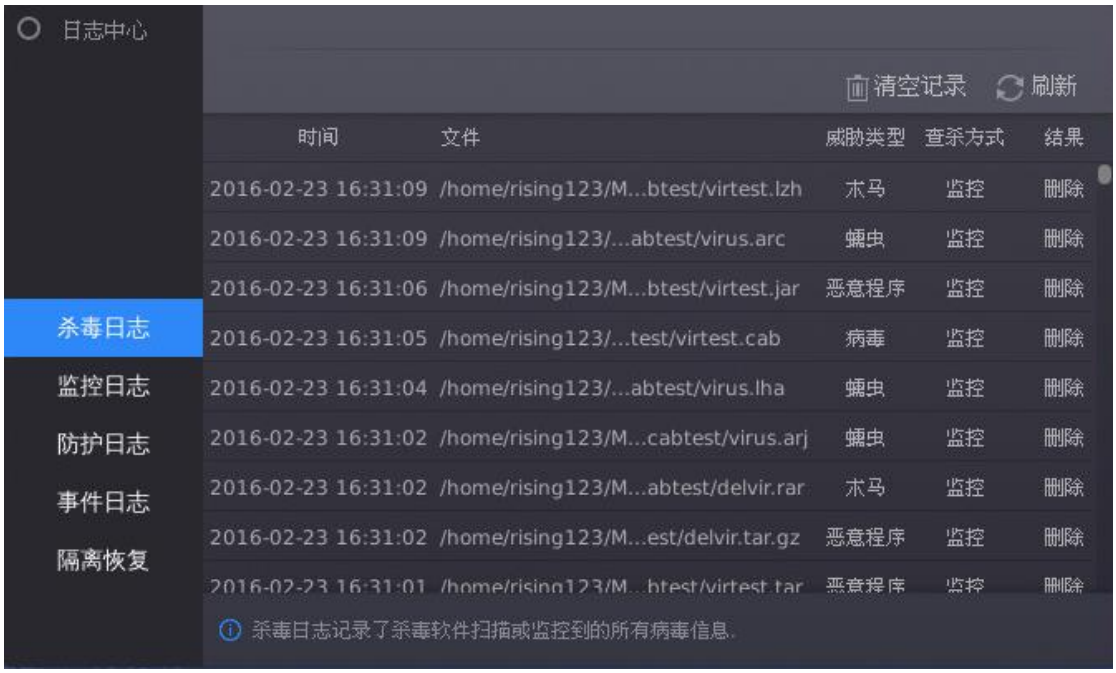
5.6.2.3.2 实时查毒功能实例

首先在“文件监控”页面列表中确认“实时查毒”功能已经开启。

图表 5-169

之后我们将有木马病毒的压缩包上传到此机器上，进行解压缩，之后发现一些文件没有了（因为是木马病毒，所以被删除了）。

然后可以到“日志中心”的“杀毒日志”中查看，发现刚才实时查毒所监控并查杀的事件日志，且所有查杀方式均为“监控”。



图表 5-170

至此我们就完成了对“实时查毒”功能的展示。

5.6.2.4 U 盘查杀

“U 盘查杀”提供木马病毒的实时监控功能，保护 USB 设备的安全接入，进行实时防护。如果 USB 设备含有木马病毒，将会被实时查杀，并记录相关日志。

5.6.2.4.1 U 盘查杀的开启及关闭

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“文件监控”模块其它功能的使用。

首先确认“文件监控”功能已经打开。

图表 5-171

之后观察右侧列表中“U 盘查杀”后面的按钮为蓝色，说明该功能已经打开。

图表 5-172

若要关闭“U 盘查杀”功能，用户可点击该蓝色开关，使其变为灰色时，此功能关闭。

图表 5-173

图表 5-174

5.6.2.4.2 U 盘查杀功能实例

首先在“文件监控”页面列表中确认“U 盘查杀”功能已经开启。

图表 5-1755

之后我们将有病毒的 U 盘插到此机器上，自动开始扫描 U 盘，之后发现一些文件没有了（因为是病毒，所以被删除了）。

然后可以到“日志中心”的“杀毒日志”中查看，就可以看到刚才实时查毒所监控并查杀的事件日志。

图表 5-176

至此我们就完成了对“U 盘查杀”功能的展示。

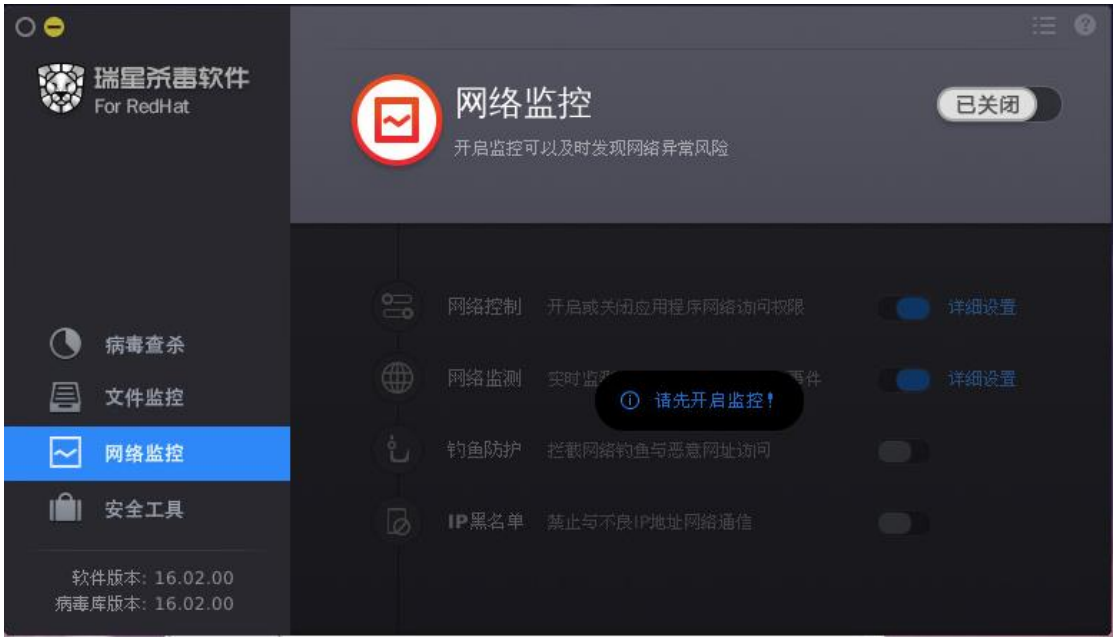
5.6.3 网络监控

“网络监控”可以对本系统正在运行的进程或可执行程序对网络的访问进行监控，可根据设置控制程序或进程对网络数据访问并记录日志。其提供的功能有：网络控制、网络监测钓鱼防护和 IP 黑名单。

注意：网络监控的全部功能都需要对瑞星杀毒软件正确进行授权后方可使用。

5.6.3.1 网络监控功能的开启及关闭

打开瑞星杀毒软件，在左列点击“网络监控”，默认“网络监控”功能没有打开。



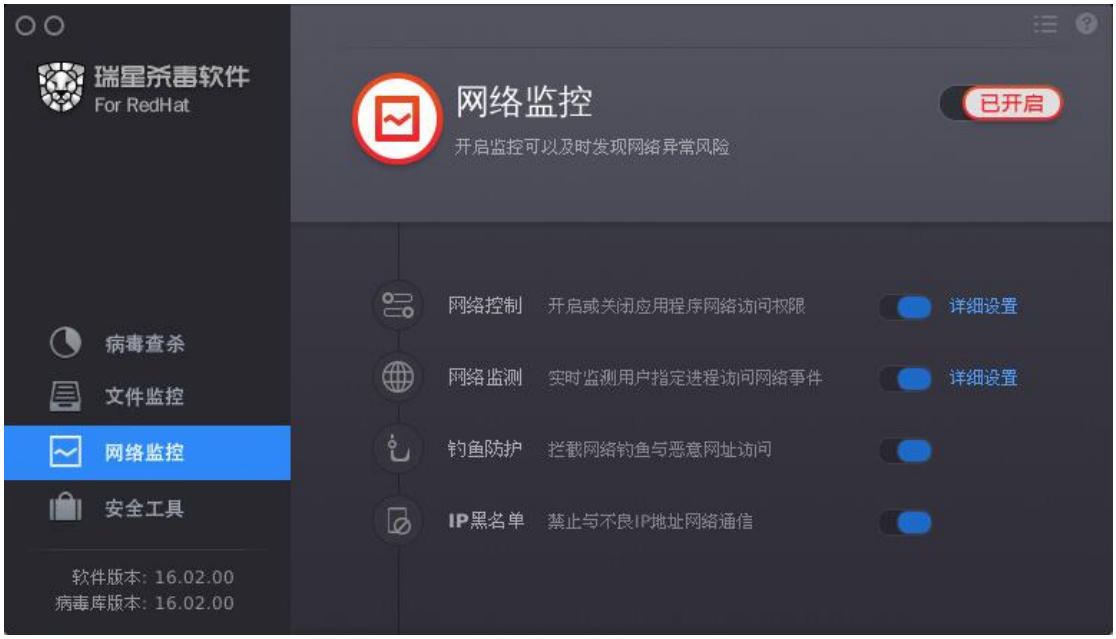
图表 5-177

可点击右侧上方“已关闭”开关，将其变为“已开启”来打开此功能。

图表 5-178

图表 5-1799

打开“网络监控”的软件界面，默认“网络控制”、“网络监测”、“钓鱼防护”和“IP 黑名单”等功能为开启状态。



图表 5-1800

注意，如果提示因授权原因无法开启此功能，请先检查软件是否已经正确分配了授权，在没有正确分配到授权时，此功能无法打开。

图表 5-1811

在“网络监控”已开启的状态下，可再次点击该开关，使其变为“已关闭”来关闭文件监控功能。

5.6.3.2 网络控制

“网络控制”允许用户添加正在运行的进程或可执行的程序，添加后，用户可控制这些程序或进程是否可以使用网络，只有用户允许使用网络的进程可以进行正常网络通信，被禁止的程序和进程将不能够访问网络。

5.6.3.2.1 网络控制的开启及关闭

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“文件监控”模块其它功能的使用。

首先确认“网络监控”功能已经打开。

图表 5-182

之后观察“网络控制”后面的开关为蓝色，说明该功能已经打开。

图表 5-1823

若要关闭“网络控制”功能，用户可点击该蓝色开关，使其变为灰色时，此功能关闭。

图表 5-1834

图表 5-1845

在“网络控制”功能为关闭状态下，若要再次打开此功能，用户只需再次点击此灰色开关，使其变为蓝色，则此功能又被打开。

5.6.3.2.2 添加或删除被控制的进程或可执行程序

用户可自行添加需要被控制的可执行程序，添加的内容可以是某个正在运行的进程，又或者是某个未运行的可执行程序。

注意：添加不可执行的程序将没有被控制效果。

首先确认“网络控制”功能已经开启。

图表 5-185

点击其后方的“详细设置”，打开“网络控制”的详细设置页面。

图表 5-186

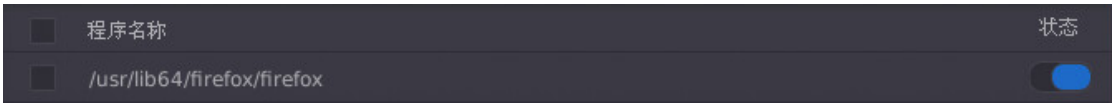
图表 5-187

点击右侧上方“添加”按钮，选择“添加进程”（这里我们假设用户已经在运行网页浏览器——火狐，进行网页浏览。）在进程窗口里找到 firefox 进程，并点击“确定”。

图表 5-188

图表 5-1890

之后用户可在“网络控制”程序列表中看到刚刚被添加的进程，且该进程的“状态”为允许访问网络（蓝色开关）。

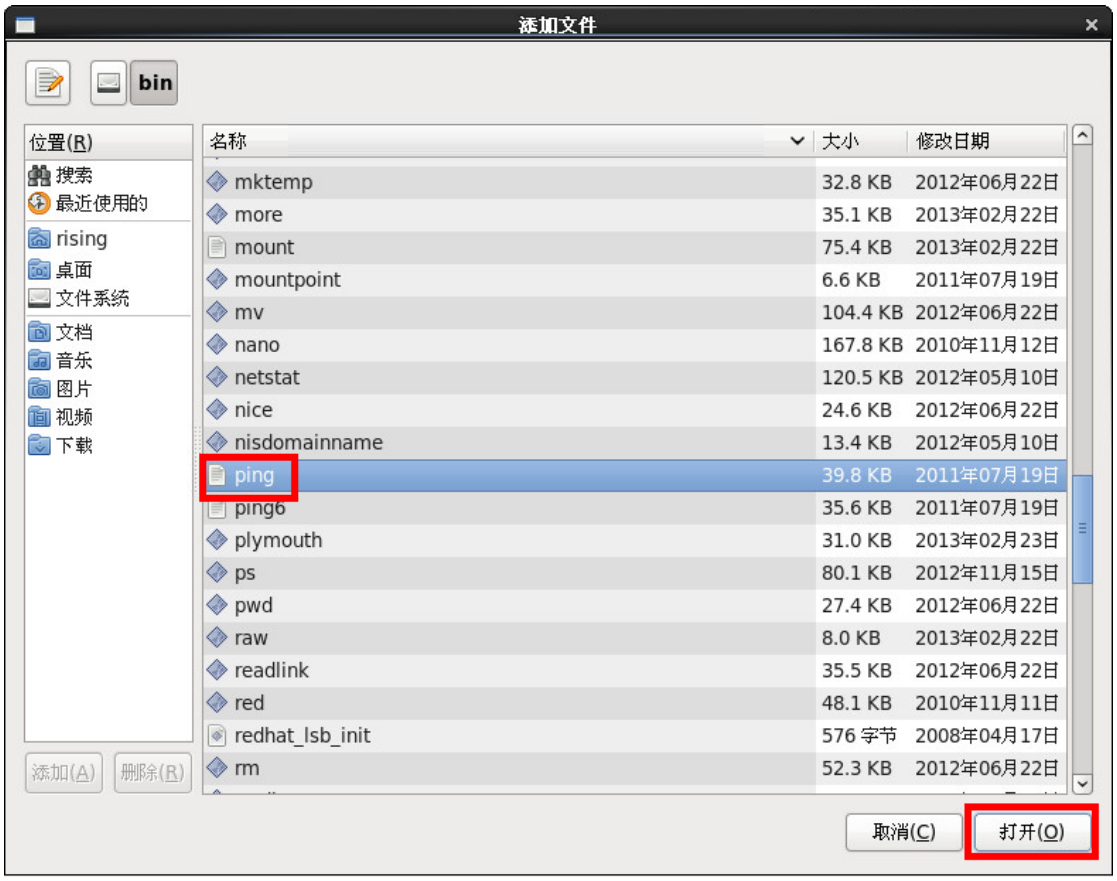


图表 5-1901

至此我们就完成了添加某个正在运行的进程到“网络控制”列表当中。

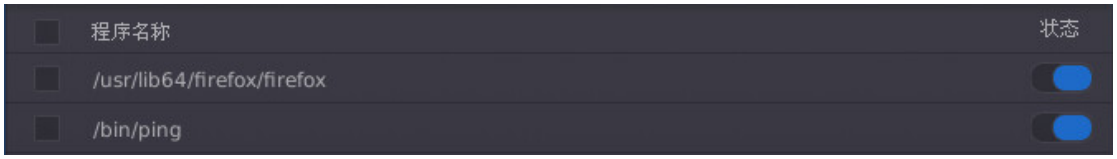
除了添加正在运行的进程，用户还可以添加某个可执行的程序到“网络控制”列表中。在“网络控制”界面点击右侧上方“添加”按钮，选择“添加文件”，打开文件浏览器，浏览并选择要添加的程序，点击右下角“打开”。

图表 5-1912



图表 5-1923

之后用户可在“网络控制”程序列表中看到刚刚被添加的程序，且该程序的“状态”为允许访问网络（蓝色开关）。

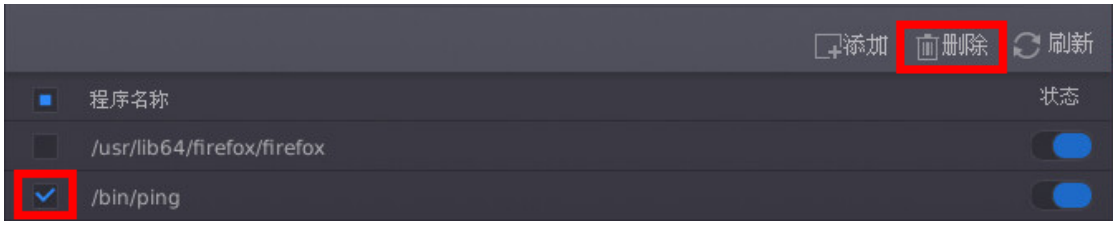


图表 5-1934

至此我们就完成了添加某个可以被执行的程序到“网络控制”列表当中。

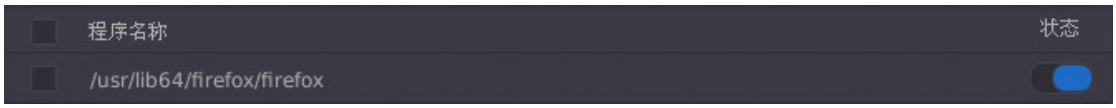
当“网络控制”列表中存在用户所添加的进程或可执行程序时，用户可选择将其从列表中删除。当列表中存在多个项目时，可以勾选多个项目进行删除。

在“网络控制”列表中，勾选要删除的进程或可执行程序，然后点击右上方的“删除”按钮。



图表 5-1945

之后，列表中被删除的项目消失。



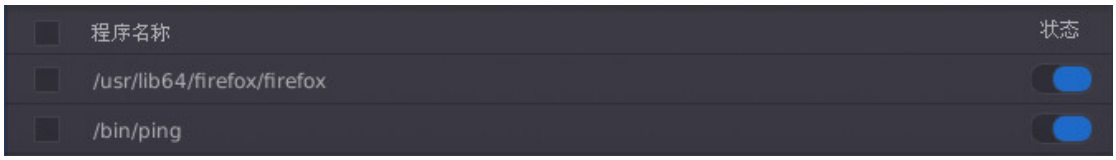
图表 5-195

至此就完成了从“网络控制”列表中删除项目。

5.6.3.2.3 允许或阻止“网络控制”项目访问网络

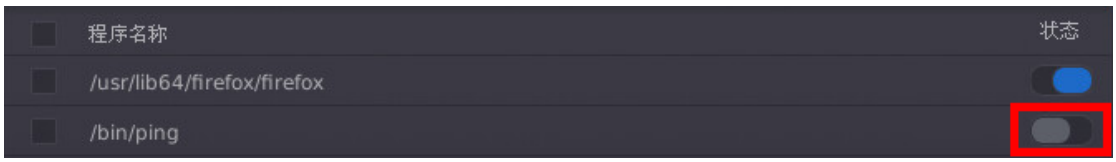
当“网络控制”列表中存在一个或多个进程或可执行程序时，用户可选择允许或阻止某个或某几个项目对网络的访问。只有允许访问（开关为蓝色）的项目可以使用网络。

当进程或程序被添加到“网络控制”列表当中时，其默认为可以使用网络（蓝色开关）。



图表 5-196

用户可点击希望阻止使用网络项目的开关，当其变为灰色时，则相应项目不能对网络进行访问。

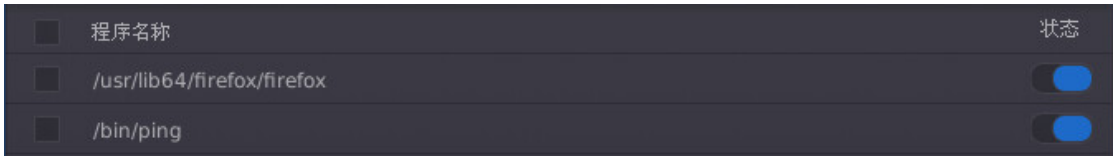


图表 5-197

对于列表中已经被阻止访问网络的项目，用户可再次点击该开关，当其变为蓝色时，相应项目又被允许访问网络。

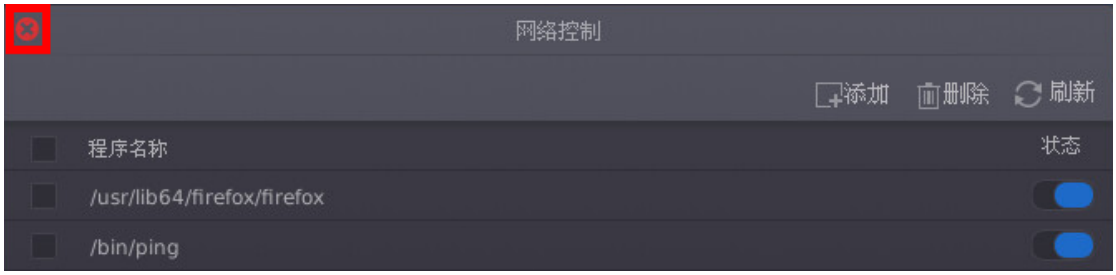
5.6.3.2.4 “网络控制”功能实例

首先在“网络控制”列表中添加想要被控制的可执行程序，（这里我们添加火狐网页浏览器 firefox，和 ping 命令），并确保其“状态”为允许访问网络（蓝色开关）。



图表 5-198

注意：当用户在列表中添加了希望被“网络控制”所控制的进程及可执行程序，或修改了某项目的状态开关后，需要点击页面左上角的X关闭此页面，才可让设置生效。



图表 5-200

之后打开火狐浏览器，浏览某网址，发现可以正常浏览网页。

图表 5-201

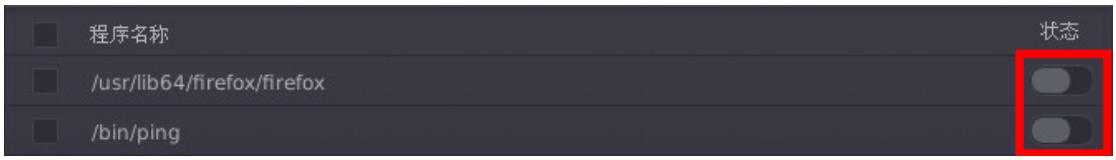
然后打开一个终端窗口，运行 ping 命令来 ping 某个内网地址，发现可以 ping 通。

```
[root@CentOS6 桌面]# ping 193.168.20.10
PING 193.168.20.10 (193.168.20.10) 56(84) bytes of data.
64 bytes from 193.168.20.10: icmp_seq=1 ttl=63 time=0.834 ms
64 bytes from 193.168.20.10: icmp_seq=2 ttl=63 time=0.669 ms
64 bytes from 193.168.20.10: icmp_seq=3 ttl=63 time=0.619 ms
64 bytes from 193.168.20.10: icmp_seq=4 ttl=63 time=0.651 ms
^C
--- 193.168.20.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3403ms
rtt min/avg/max/mdev = 0.619/0.693/0.834/0.085 ms
```

图表 5-19902

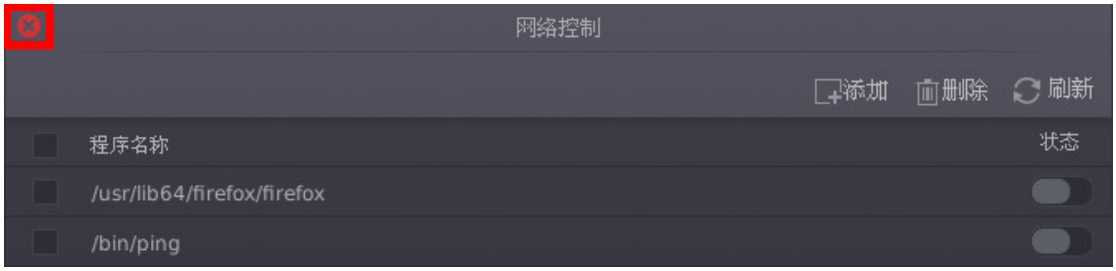
这说明当允许“网络控制”中的项目访问网络时（蓝色开关），该项目均可正常访问网络。

然后我们在“网络控制”列表中，分别点击此两项目后的“状态”开关，将其变为灰色（即禁止相应项目访问网络）。



图表 5-203

之后点击左上角“X”关闭“网络控制”详细设置页面以使设置生效。



图表 5-204

然后我们再次用此机器上的火狐浏览器浏览网页，发现无法进行浏览。

图表 5-20005

再次在终端窗口中用 ping 命令，发现无法 ping 通任何地址。

```
[root@CentOS6 桌面]# ping 193.168.20.10
connect: 成功
[root@CentOS6 桌面]#
```

图表 5-201

这说明当阻止“网络控制”中的项目访问网络时（灰色开关），该项目不能访问网络。

5.6.3.3 网络监测

“网络监测”功能可以根据用户所设定的配置记录那些正在运行的进程或可执行文件对网络的使用事件。所有事件日志都将记录在“日志中心”的“监控日志”当中。

5.6.3.3.1 “网络监测”的开启及关闭

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“文件监控”模块其它功能的使用。

首先确认“网络监控”功能已经打开。

图表 5-202

之后观察“网络监测”后面的开关为蓝色，说明该功能已经打开。

图表 5-203

若要关闭“网络监测”功能，用户可点击该蓝色开关，使其变为灰色时，此功能关闭。

图表 5-204

图表 5-2050

在“网络监测”功能为关闭状态下，若要再次打开此功能，用户只需再次点击此灰色开关，使其变为蓝色，则此功能又被打开。

5.6.3.3.2 添加或删除被监测的进程或可执行程序

用户可自行添加需要被监测的可执行程序，添加的内容可以是某个正在运行的进程，又或者是某个未运行的可执行程序。

注意：添加不可执行的程序将没有被监测效果。

首先确认“网络监测”功能已经开启。

图表 5-2061

点击其后方的“详细设置”，打开“网络监测”的详细设置页面。

图表 5-2072

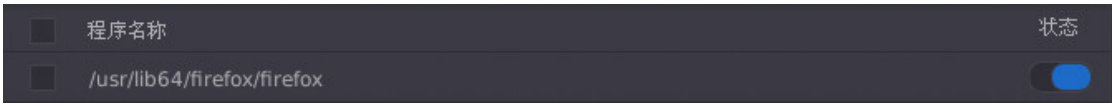
图表 5-2083

点击右侧上方“添加”按钮，选择“添加进程”（这里我们假设用户已经在运行网页浏览器——火狐，进行网页浏览。）在进程窗口里找到 firefox 进程，并点击“确定”。

图表 5-2094

图表 5-2105

之后用户可在“网络监测”程序列表中看到刚刚被添加的进程，且该进程的“状态”为记录对网络访问（蓝色开关）。



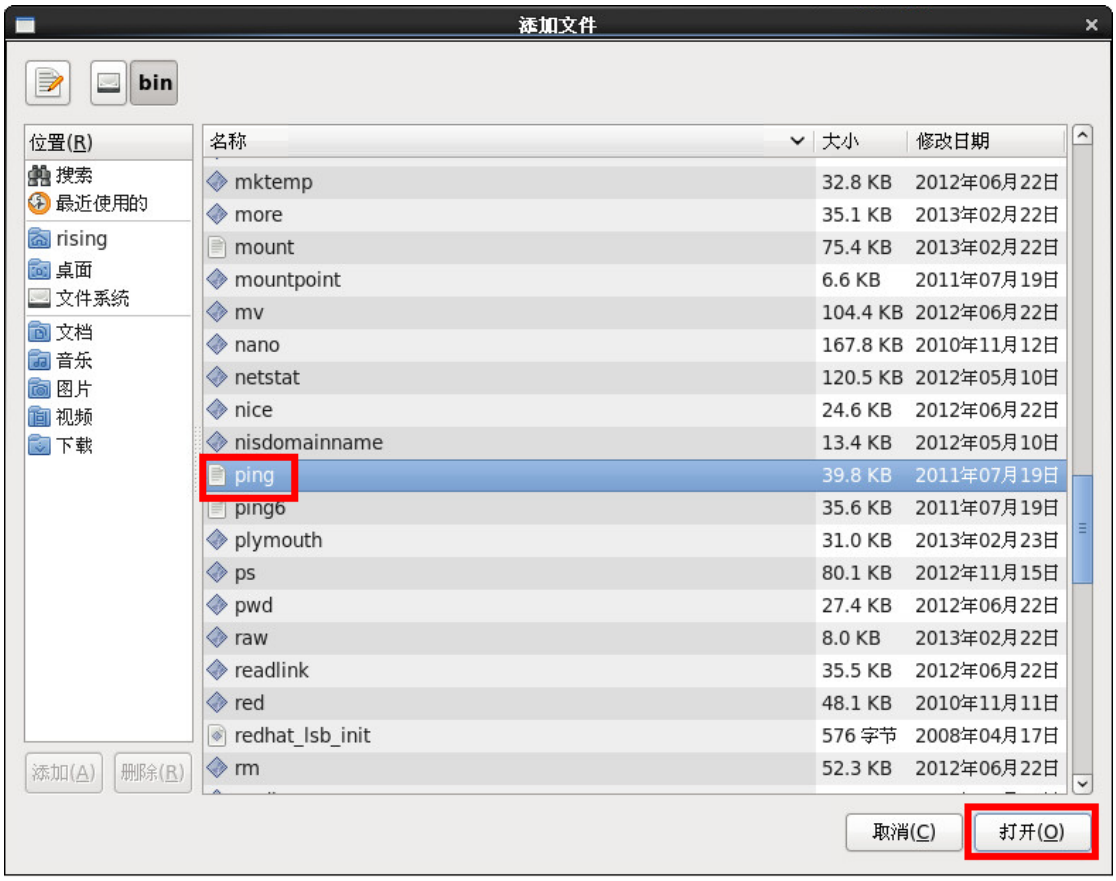
图表 5-211

至此我们就完成了添加某个正在运行的进程到“网络监测”列表当中。

除了添加正在运行的进程，用户还可以添加某个可以被执行的程序到“网络监测”列表中。

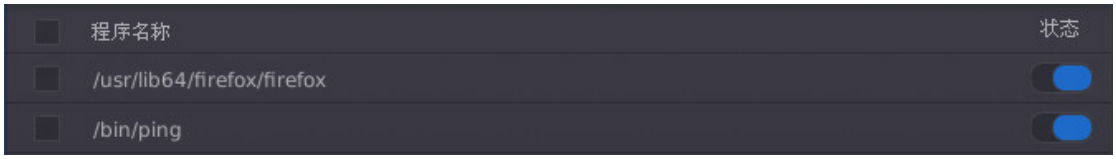
点击右侧上方“添加”按钮，选择“添加文件”，打开文件浏览器，浏览并选择要添加的程序，点击右下角“打开”。

图表 5-212



图表 5-213

之后用户可在“网络监测”程序列表中看到刚刚被添加的程序，且该程序的“状态”为记录对网络访问（蓝色开关）。

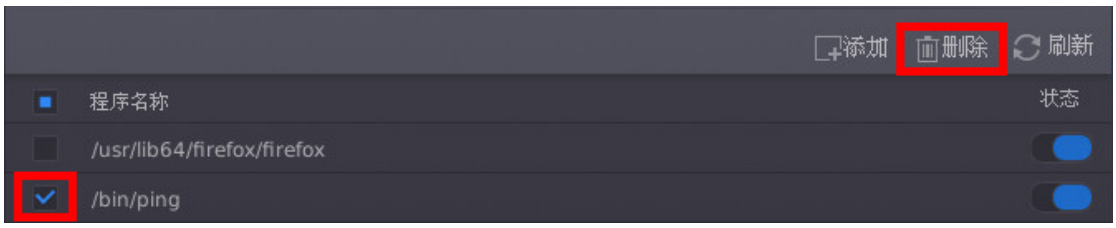


图表 5-214

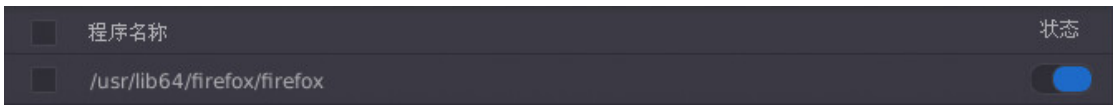
至此我们就完成了添加某个可以被执行的程序到“网络监测”列表当中。

当“网络监测”列表中存在用户所添加的进程或可执行程序时，用户可选择将其从列表中删除。当列表中存在多个项目时，可以勾选多个项目进行删除。

在“网络监测”列表中，勾选要删除的进程或可执行程序，然后点击右上方的“删除”按钮。



图表 5-2150



图表 5-2161

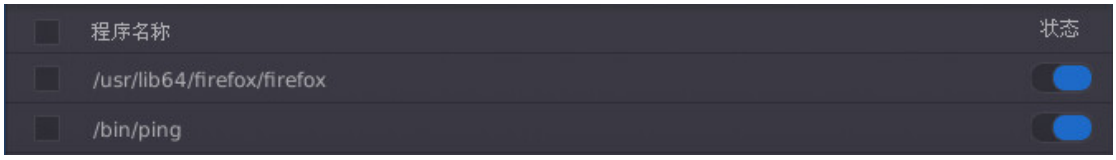
之后，列表中被删除的项目消失。

至此就完成了从“网络监测”列表中删除项目。

5.6.3.3.3 打开或关闭对程序访问网络的监测记录

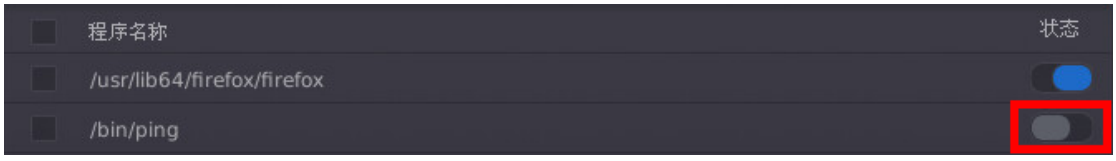
当“网络监测”列表中存在一个或多个进程或可执行程序时，用户可选择打开或关闭监测某个或某几个项目对网络的访问记录。当某项目后的“状态”开关为蓝色时，网络监测将会记录该项目对网络的访问事件。

当进程或程序被添加到“网络监测”列表当中时，其默认为打开对该项目的网络访问记录（蓝色开关）。



图表 5-2172

用户可点击希望关闭记录使用网络项目的“状态”开关，当其变为灰色时，则不会记录相应项目对网络访问的事件。

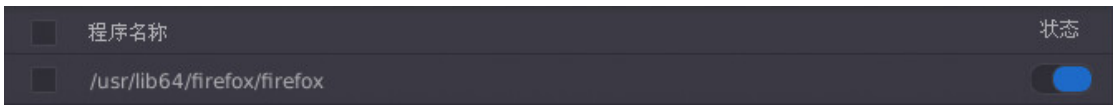


图表 5-2183

对于列表中已经关闭记录访问网络的项目，用户可再次点击该开关，当其变为蓝色时，又开始记录相应项目访问网络的事件。

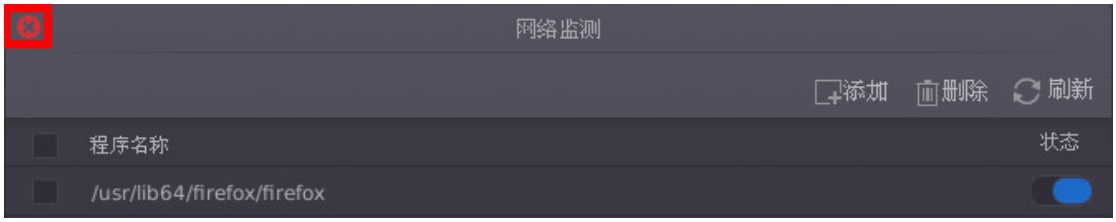
5.6.3.3.4 “网络监测”功能实例

首先在“网络监测”列表中添加想要被监测的可执行程序，（这里我们添加火狐网页浏览器 firefox），并确保其“状态”为记录该项目对网络的访问事件（蓝色开关）。



图表 5-2194

注意：当用户在列表中添加了希望被“网络监测”所监测的进程及可执行程序，或修改了某项目状态开关后，需要点击页面左上角的X关闭此页面，才可让设置生效。



图表 5-2205

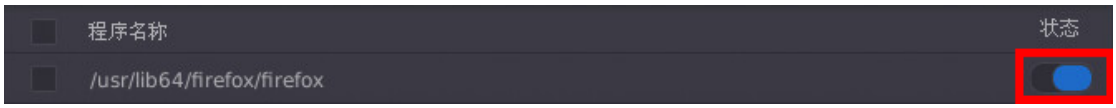
之后打开火狐浏览器，浏览某网址，发现可以正常浏览网页。

图表 5-221

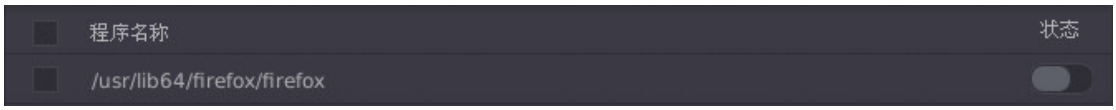
然后查看“日志中心”的“监测日志”，发现有刚才用火狐历览器浏览网站的详细记录。

图表 5-222

如果希望关闭对火狐浏览器访问网络的监控记录，用户只需在“网络监测”“详细设置”列表中点击该项目“状态”开关，使其变为灰色。



图表 5-223



图表 5-224

之后点击左上角“X”关闭“网络监测”详细设置页面以使设置生效。

图表 5-2250

然后我们再次用此机器上的火狐浏览器浏览网页的访问，均不会被“网络监测”所记录。

5.6.3.4 钓鱼防护

“钓鱼防护”可以允许用户设置恶意网址名单，阻止与列表中的网址通信。

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“网络监控”模块其它功能的使用。

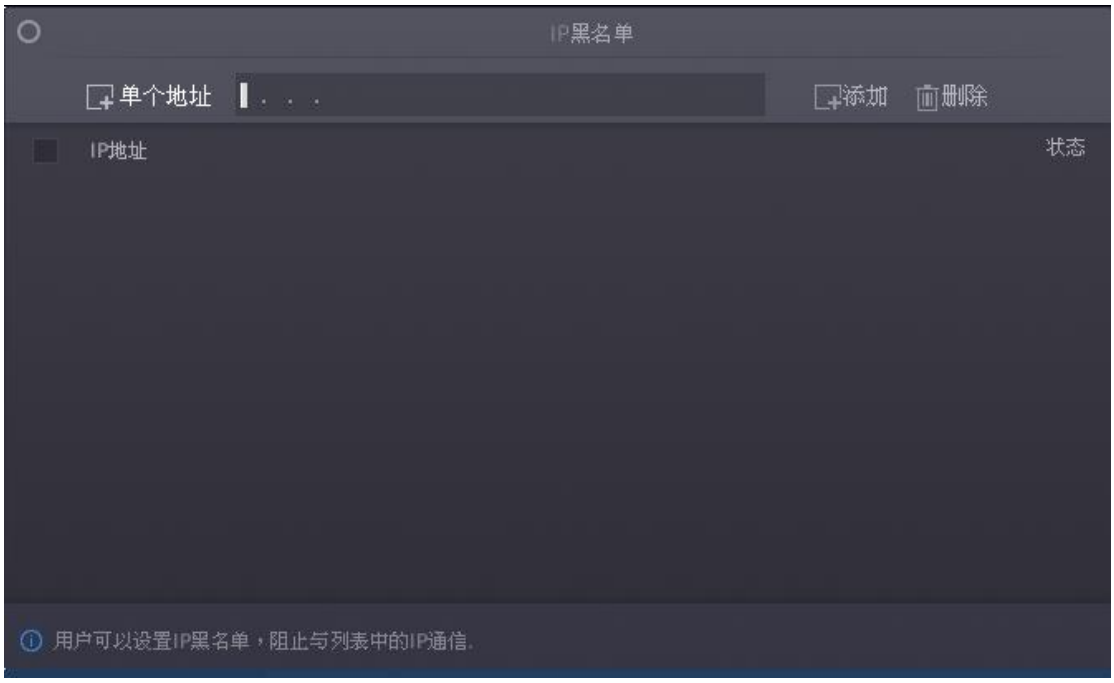
图表 5-231

5.6.3.5 IP 黑名单

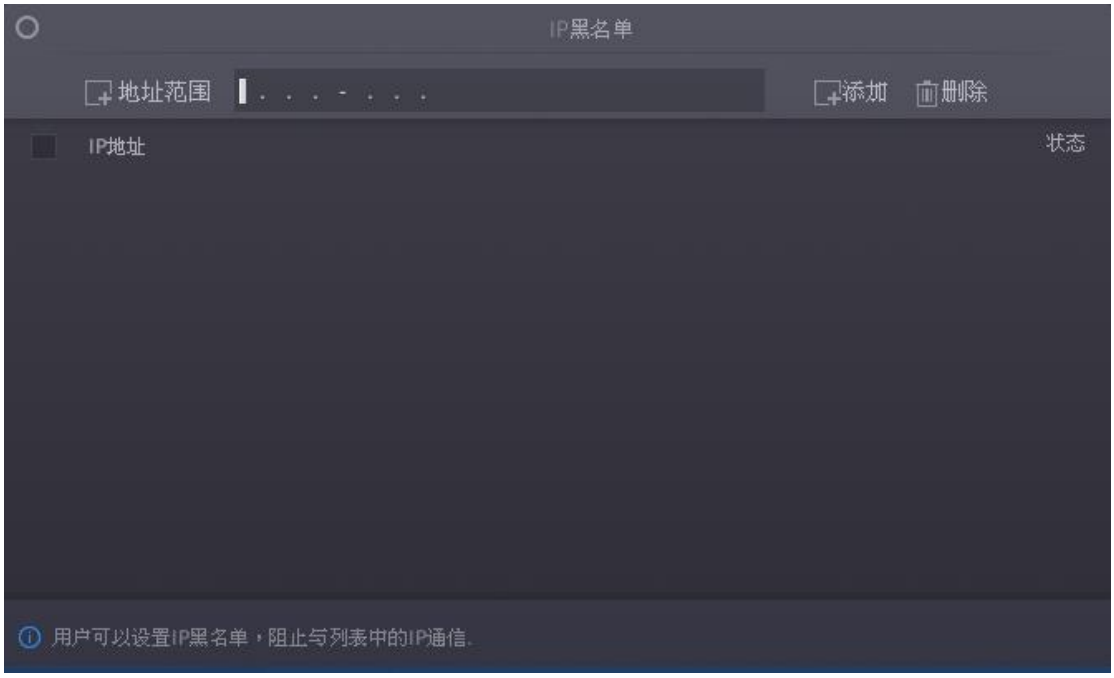
“IP 黑名单”可以允许用户设置 IP 黑名单，阻止与列表中的 IP 通信。

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“网络监控”模块其它功能的使用。

设置 IP 黑名单时，不仅可以设置单个地址，还可以设置地址范围。



图表 5-2262



图表 5-2273

5.6.3.6 IPS/IDS

“IPS/IDS”监测并阻止黑客或病毒对本系统发起的网络攻击。

用户可自行选择是否打开此功能，此功能的打开或关闭不影响“网络监控”模块其它功能

的使用。

“IPS/IDS”显示 SQL 防注入专家规则数据。

图表 5-2284

5.6.4 安全工具

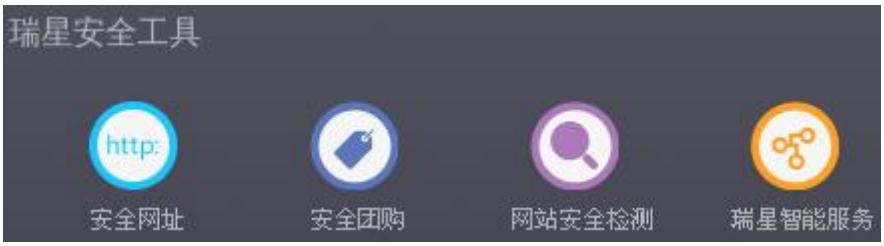
安全工具可为用户提供方便、安全的软件或相关服务，包括“瑞星安全工具”和“系统使用工具”。

用户可在瑞星杀毒软件 for Linux 的主界面点击左列“安全工具”来打开“安全工具”界面。

图表 5-2295

5.6.4.1 瑞星安全工具

瑞星安全工具是瑞星公司在日常所积累的可以方便用户进行安全的日常工作及网络通信的软件工具集合，包括“安全网址”、“安全团购”、“网站安全检测”和“瑞星智能服务”。



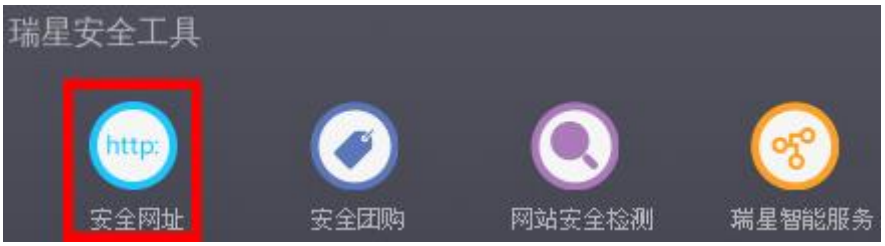
图表 5-2306

5.6.4.1.1 安全网址

“安全网址”是瑞星公司经过平日的积累，将用户日常经常会用到的，并且为安全的网址加以集中展现，是方便用户日常网络访问的安全入口。

图表 5-2317

用户可在瑞星杀毒软件 for Linux 的“安全工具”页面，点击右侧“瑞星安全工具”下的“安全网址”，来打开该网页，从上面选择安全的网址进行浏览。



图表 5-232

之后浏览器将会自动打开“安全网址”页面供用户浏览。

注意：浏览页面要求用户系统可以连接到互联网。

图表 5-233

5.6.4.1.2 安全团购

“安全团购”是瑞星所统计的真实有效的团购信息，可方便用户进行网络团购活动。

图表 5-2340

用户可在瑞星杀毒软件 for Linux 的“安全工具”页面，点击右侧“瑞星安全工具”下的“安全团购”来打开该网页，从上面选择感兴趣的团购信息进行浏览。

图表 5-2351

之后浏览器将会自动打开“安全团购”页面供用户浏览。

注意：浏览页面要求用户系统可以连接到互联网。

图表 5-2362

5.6.4.1.3 网站安全检测

“网站安全检测”是瑞星通过多年专业的积累，为各类网站提供可靠的安全评估检测，其主要项目包括：密码安全检测、网站漏洞检测、网站挂马检测、跨站脚本，和 sql 注入等网站相关安全的专业检测，是每个站长的得力助手。

图表 5-2373

用户可在瑞星杀毒软件 for Linux 的“安全工具”页面，点击右侧“瑞星安全工具”下的“网站安全检测”，来打开该网页，从上面选择感兴趣的网站安全检测项目进行安全检测。

注意：浏览页面要求用户系统可以连接到互联网。

图表 5-2384

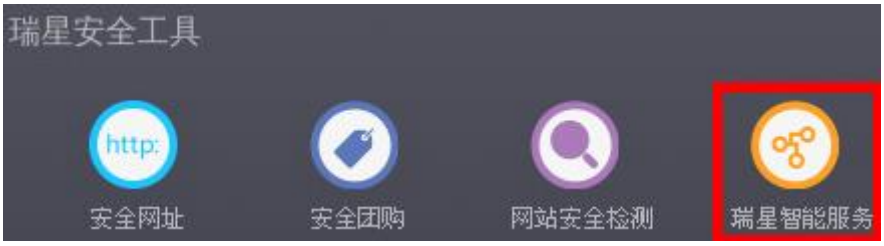
5.6.4.1.4 瑞星智能服务

“瑞星智能服务”是用智能软件解答的方式替代以往需要人工客服来解答的一些瑞星软

件中使用的常见问题，其可在没有人工干预的情况下，智能的根据用户提出的问题给出相应的答案，有助于帮助用户解决在使用瑞星软件产品过程中碰到的问题。

图表 5-2395

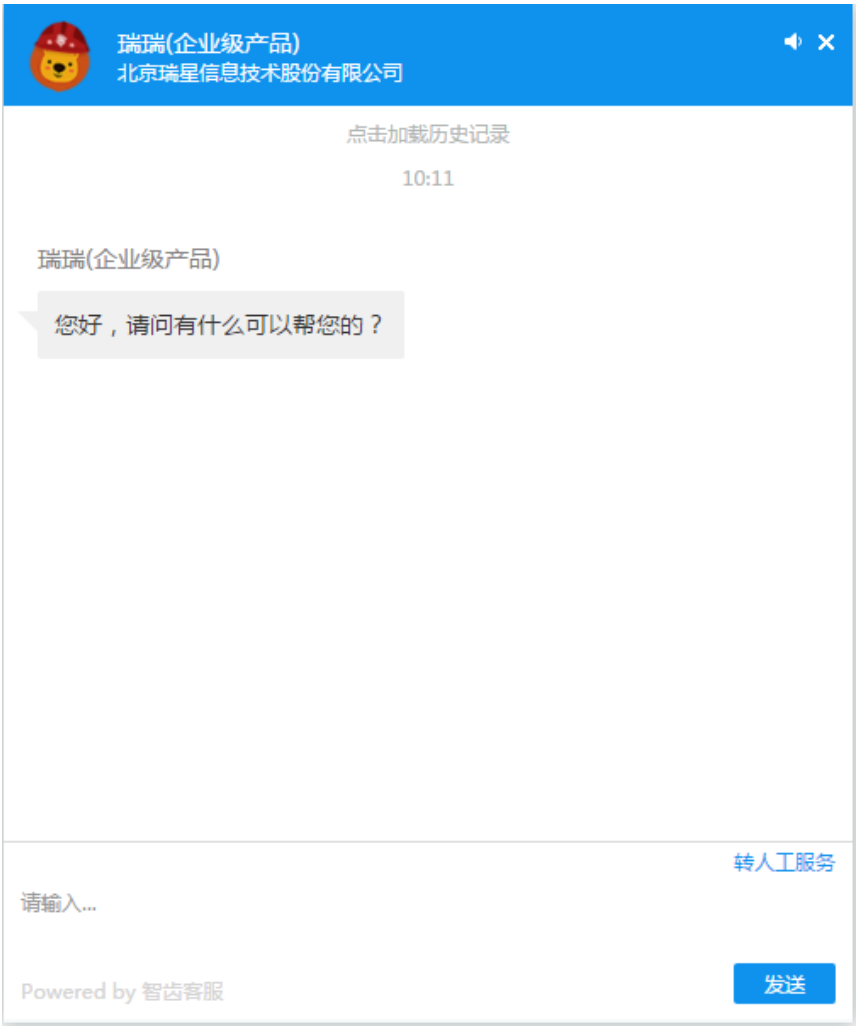
用户可在瑞星杀毒软件 for Linux 的“安全工具”页面，点击右侧“瑞星安全工具”下的“瑞星智能服务”来打开该网页，输入自己使用软件碰到的问题，并获得解答。



图表 5-2406

之后浏览器将会自动打开“瑞星智能服务”页面供用户浏览。

注意：浏览页面要求用户系统可以连接到互联网。



图表 5-241

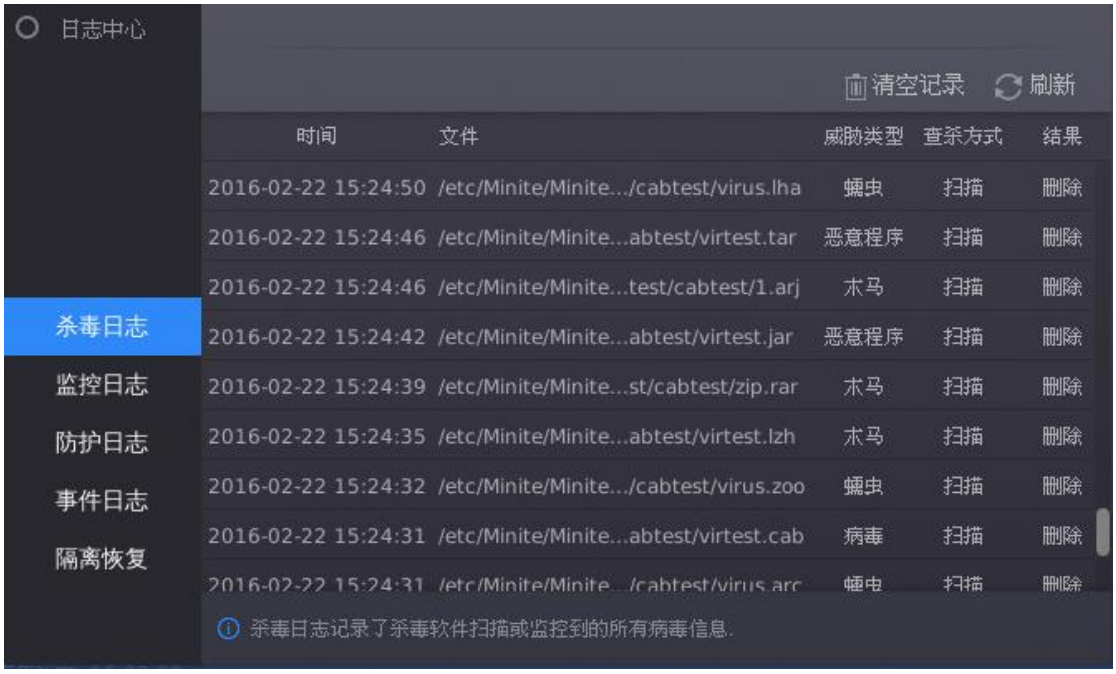
5.6.5 日志中心

日志中心是用户查看软件各类日志的场所，用户可在瑞星杀毒软件界面右上角点击“菜单”按钮。

图表 5-242

然后点击“日志中心”来打开“日志中心”界面。

图表 5-243



图表 5-2440

日志中心包括 “杀毒日志”、“监控日志”、“防护日志”、“事件日志”和“隔离恢复”。

5.6.5.1 杀毒日志

“杀毒日志”记录了杀毒软件监控或扫描所发现的木马病毒等风险程序，用户可在此处查看杀毒软件所发现的所有木马病毒等风险程序，用户可在“日志中心”界面点击左列“杀毒日志”来打开杀毒日志界面。

图表 5-2451

其中主要记录了发现木马病毒的时间、感染文件、威胁类型、查杀方式和处理结果等内容。

5.6.5.2 监控日志

“监控日志”记录了在“网络监测”中所设置的监控项目（如监控浏览器程序对网络访问的记录）。

用户可在“日志中心”界面点击左列“监控日志”来打开其界面。

图表 5-2462

其中主要记录了被监测程序或进程访问网络的时间，进程名称，使用的协议，以及详情描述等内容。

5.6.5.3 防护日志

“防护日志”记录了软件“自我保护”功能所拦截的未经授权擅自尝试删除或篡改杀毒软件的事件。用户可在“日志中心”界面点击左列“防护日志”来打开其界面。

图表 5-2473

其中主要记录了尝试删除或篡改杀毒软件的时间、进程名称、尝试操作、以及被保护文件和处理结果等内容。

5.6.5.4 事件日志

“事件日志”中记录了用户发起的扫描任务事件，用户可在“日志中心”界面点击左列点击“事件日志”来打开其界面。

图表 5-2484

其中主要记录了用户发起扫描任务的时间、事件（采用何种方式扫描），以及扫描详情等内容。

5.6.5.5 隔离恢复

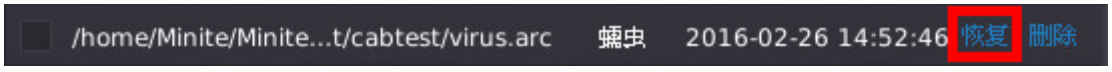
“隔离恢复”中记录了杀毒软件所处理过的木马病毒。用户可在“日志中心”界面点击左列“隔离恢复”来打开该界面。

图表 5-2495

其中主要记录了被隔离文件的路径及名称、处理原因、处理时间和可供用户的操作选项（包括恢复和删除）。

5.6.5.5.1 恢复隔离区文件

用户可选择恢复一个或多个隔离区文件，当“隔离恢复”列表中存在隔离文件时，用户可点击该项目后方的“恢复”按钮，将此文件恢复到原位置。



图表 5-2506

该项目被恢复后从“隔离恢复”列表中消失。

图表 5-251

用户还可以一次“勾选”一个或多个文件，然后点击页面上方的“恢复所选”一次恢复一个或多个文件。

图表 5-252

项目被恢复后从“隔离恢复”列表中消失。

图表 5-253

注意：为了避免被恢文件再次被查杀，用户选择恢复的文件，将自动添加到“可信文件”列表，用户可在“系统设置”中的“可信文件”中看到这些文件。

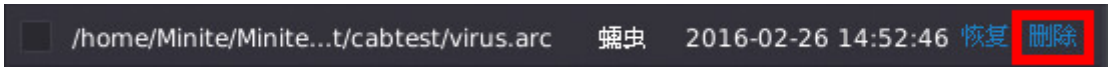
图表 5-2540

5.6.5.5.2 删除隔离文件

用户可选择删除一个或多个隔离文件，当“隔离恢复”列表中存在隔离文件时，用户可点

击该项目后方的“删除”按钮，将此文件从隔离区删除。

注意：删除的文件将不能再恢复。

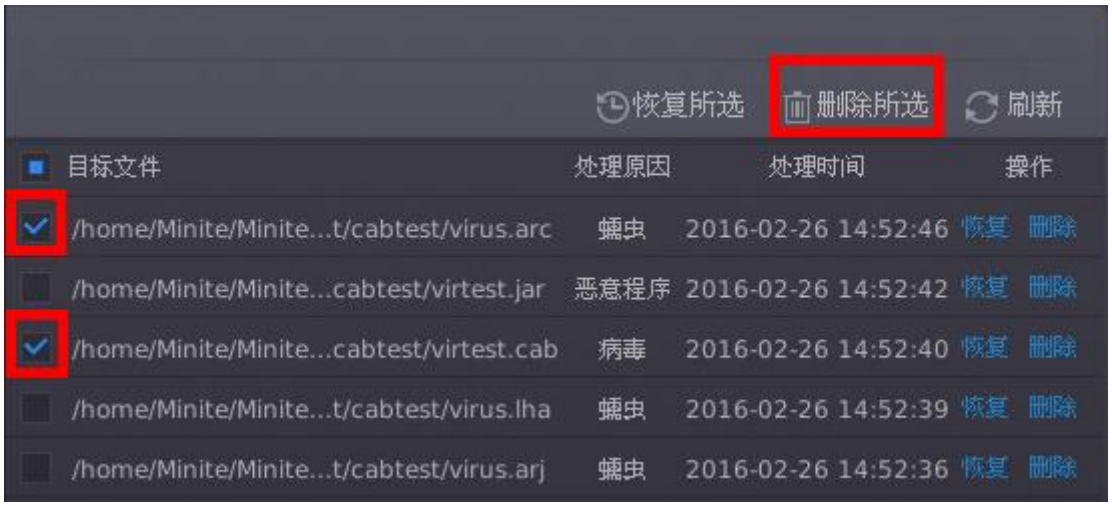


图表 5-2551

该项目被删除后从“隔离恢复”列表中消失。

图表 5-2562

用户还可以一次“勾选”一个或多个文件，然后点击页面上方的“删除所选”一次删除一个或多个文件。



图表 5-2573

项目被删除后从“隔离恢复”列表中消失。

图表 5-2584

5.6.5.6 日志的刷新及删除

5.6.5.6.1 日志的刷新

在“杀毒日志”、“监控日志”、“防护日志”或“事件日志”当中，用户可点击页面右上角的“刷新”按钮来实时刷新日志状态。

图表 5-2595

点击“刷新”后，若有新的日志记录，将出现在日志列表当中。

5.6.5.6.2 清空日志记录

在“杀毒日志”、“监控日志”、“防护日志”或“事件日志”当中，用户可点击页面右上角的“清空记录”按钮来手动清空该项目日志记录。

图表 5-2606

点击“清空记录”后，该项目所有日志被清空。

图表 5-261

附录一 北京瑞星信息技术股份有限公司简介

瑞星公司主营业务为信息安全整体解决方案的研发、销售及相关增值服务。公司自成立以来一直专注于信息安全领域，以优质的产品和专业的“安全+”服务，向政府、企业及个人提供基于桌面安全、边界安全、管理安全、审计安全、移动安全、虚拟化安全等核心技术的整体解决方案，帮助所有用户有效应对各种类型的信息安全威胁。

公司的主要业务包括企业及个人两大部分。企业级业务涉及：企业终端安全防护、企业网络边界防护、企业网络安全预警、企业网络监测、企业信息审计、虚拟化信息安全、云存储安全、企业移动安全、企业信息安全检测、企业信息安全培训、企业数据恢复、应急响应服务等领域。个人级业务涉及：个人电脑终端安全、个人移动安全、个人网络边界防护、个人数据恢复等领域。

瑞星公司是具有认证资质的高新技术企业，承担了我国第一个虚拟化反病毒国家实验室的建设，并承接了我国第一例虚拟化云存储项目的信息安全建设工作，具有雄厚的技术实力。此外，依托二十余年坚持不懈的产品技术创新和项目经验积累，瑞星在国内信息安全市场中赢得了良好的声誉及口碑。

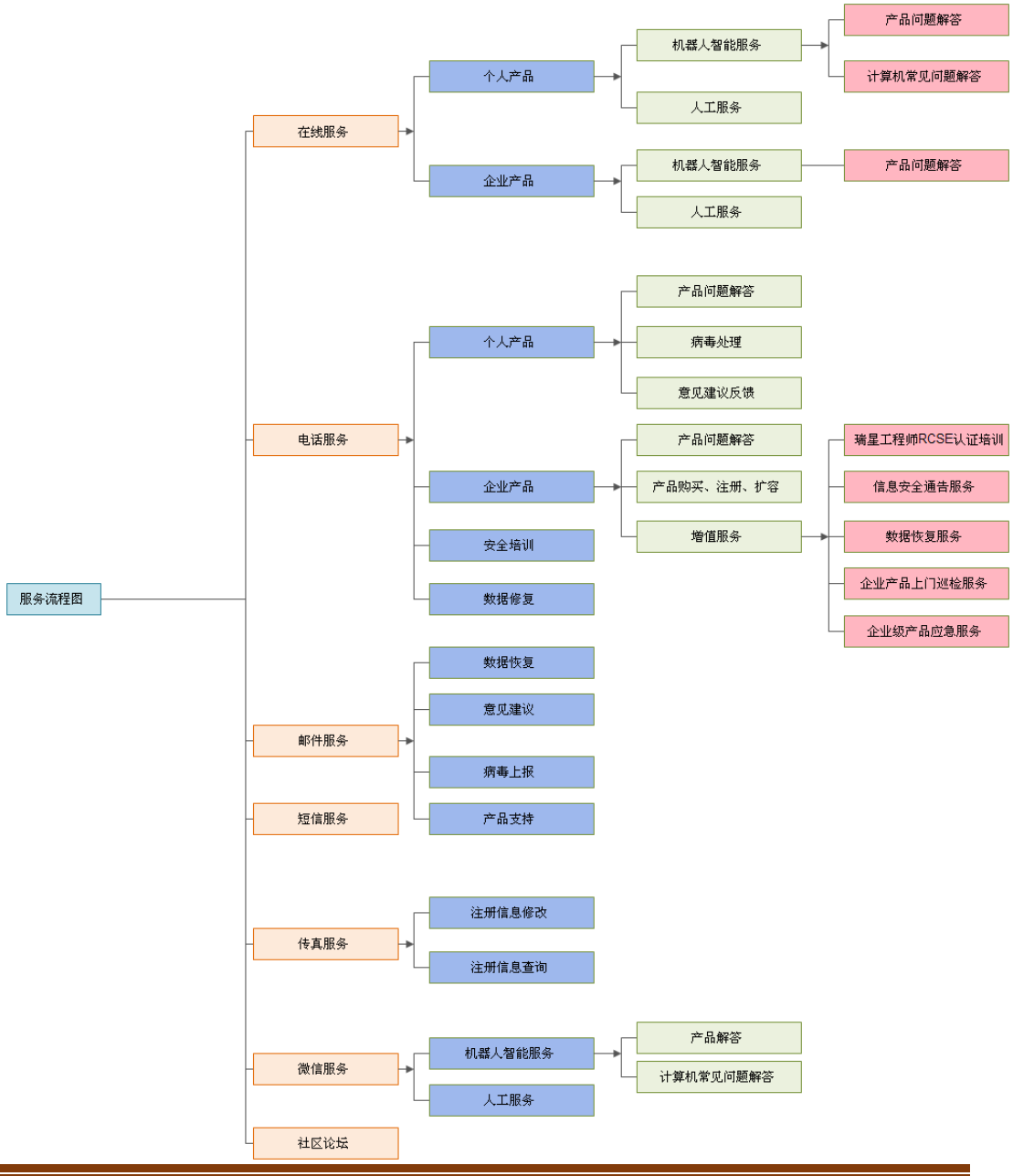
未来，受“互联网+”计划影响，国内所有传统企业都将大幅向互联网模式转变，信息安全将成为决定企业生存发展的重要因素。因此，瑞星根据多年的技术经验积累，以云计算安全、大数据安全、移动安全、桌面安全、边界安全为基础，为“互联网+”下的企业量身打造了一套“企业信息安全+”整体解决方案，力争为所有企业用户提供最安全最便捷的信息安全保障。

附录二 客户服务简介

一、 服务体系说明

瑞星公司拥有百余位专业信息安全工程师通过在线服务、电话服务、邮件服务、短信服务、传真服务、微信服务及社区论坛等多种服务方式为您提供全面、专业、及时的技术支持与安全解决方案。

您可参照以下服务体系及其服务流程进行问题咨询和求助。



二、 服务方式介绍

1. 在线服务

智能服务（7 x 24）：

瑞星公司引入了目前最先进的智能机器人服务系统，通过“智能服务+人工服务”的全新服务模式，给用户提供最专业、最全面的问题解答。

现在点击瑞瑞的头像来尝试和瑞瑞聊天吧！当然您还可以访问瑞星客服中心网站(http://csc.rising.com.cn/index.html)，根据您使用的产品选择相应的在线服务，瑞星智能机器人“瑞瑞”会 7 x 24 小时全天解答您的任何问题。

·人工服务（5 x 8）：

当您遇到特殊问题需要与瑞星工程师咨询反馈时，您可以在机器人瑞瑞的聊天界面中选择“转人工服务”直接与工程师沟通。

2. 电话服务

2004 年瑞星公司斥资 500 万建设业内第一个"电信级"呼叫中心，2007 年再次投资 1500 万元扩建呼叫中心，2009 年开通 400 服务热线为客户提供更优质服务

客户服务电话：400-660-8866 (免长途话费)

北京及未开通 400 电话地区：010-82678800（个人级）010-82616666（企业级）

3. 邮件服务

您可以访问邮件服务中心(http://mailcenter.rising.com.cn)，发送咨询邮件获得专业指导。

4. 短信服务

短信客服号码：106575020236

短信服务是针对瑞星用户提供的特色服务，您可通过短信获得技术支持，此服务目前仅针对中国移动用户提供。

手机里输入您要咨询的内容，发送短信至 106575020236，瑞星工程师会在工作日内即时回答您的问题。

5. 传真服务

个人级产品：010-82678800（请根据语音提示选择对应数字键进行传真）

企业级产品：010-82616666-8

6. 微信服务

瑞星客户服务中心微信号：Rising-Service

您可以使用手机微信搜索“瑞星客服”或“Rising-Service”，也可以直接扫描二维码添加瑞星客服公众号，在公众号右下角菜单的“更多”中选择“智能客服”，随时随地咨询瑞星相关问题。

7. 社区论坛

论坛服务：http://bbs.ikaka.com/

访问卡卡安全论坛，解决产品使用中遇到的问题，获取最新问题解决方案。

三、 增值服务

(一)信息安全预警服务

1、 短信通报和邮件通报

通过短信和邮件发送最新安全动态、病毒、漏洞等信息，使各企事业单位信息安全管理员获取最专业权威的资讯，并提前消除网络中的安全威胁，排除安全隐患。

2、 挂马网站预警

当用户的 WEB 网站被遭到挂马攻击，系统会自动通知用户网站管理员进行处理，避免产生严重后果。

(二)信息安全专家服务

1、 专属电话通道

用户加入 VIP 客户电话通道后，拨打客服热线，可优先接入，遇忙转接至指定高级工程师，享受问题咨询优先受理。

2、 信息安全顾问

为企业客户指定“一对一”安全顾问提供服务，针对该企业的网络结构、管理要求、网络安全要求等实际情况，提供有针对性的防毒产品部署、配置方案。

3、 光盘邮寄

针对特殊网络环境、上网不方便、管理要求严格的客户，提供加密光盘邮寄服务，光盘内容包括产品安装程序、升级程序、引导杀毒映像、使用手册、技术白皮书、产品解决方案等个性化内容。

(三)信息安全响应服务

1、 现场巡检

指定高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供上门巡检服务，服务内容包括：产品使用培训、产品运行检测、病毒日志分析、现场技术支持等服务，并提供内容可定制的巡检报告。

2、 远程巡检

由指定的高级安全顾问与客户建立紧密的长期合作关系，定期为客户提供远程巡检服务，服务内容包括：产品运行检测、病毒日志分析、远程技术支持等服务吗，可提供内容定制的巡检报告。

3、 现场紧急救援

针对在发生突发性问题（如：病毒、网络和瑞星产品等问题）时提供及时现场技术支持，提供解决方案并协助解决问题，根据路线可在 1-3 小时内抵达现场。

4、 远程紧急救援

通过远程工具、远程桌面或瑞星企业版用户在线服务等方式针对发生突发性问题（如：病毒、网络和瑞星产品等问题）时提供技术支持，为用户提供解决方案并协助用户第一时间

解决问题。

5、 数据灾难恢复

当存储介质出现损伤或由于误操作、病毒导致磁盘数据丢失或损坏的情况。数据灾难恢复服务将帮助客户挽救数据，挽回损失。

(四)信息安全培训服务

从日常网络安全维护、防火墙应用、流行病毒处理、网络攻击应对以及危机发生处理等等方面进行全方面的培训。包括电脑安全使用基础培训、计算机反病毒普及培训、网络安全工程师认证培训、网络管理员高级培训等等，也可以根据企业个性化需求定制培训。

服务须知

了解更多增值服务细节或购买请咨询 400-660-8800(010-82616666)或访问瑞星客户服务中心(http://csc.rising.com.cn/index.html)。

四、 联系方式

工作时间：国家法定工作日 9:00-17:30

联系地址：北京市海淀区中关村大街 22 号中科大厦 1403 室

邮政编码：100190