重要声明

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

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

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

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

忠告用户

- (1)请将所购产品与"产品组件清单"进行核对,以确定产品的完整性。确认 购买的产品为瑞星公司的正版产品;
- (2)如果自购买日起一个月后未注册,将不能得到包括升级在内的技术支持和 售后服务;
- (3)为了避免"产品序列号"、"授权证书"等机密信息泄露,保障用户的合 法权益不受侵害,瑞星公司不接受除了最终用户以外的任何人或机构的代替 注册;
- (4) 请准确填写注册中的每项内容并及时注册;
- (5)请妥善保管"产品序列号"和"授权证书",以免软件被盗用,从而影响 自己的正常使用;
- (6)如对产品包装内物品和注册过程有疑义,请立即向该套产品的提供商或瑞 星公司咨询;
- (7)任何情况下,不得在授权范围外使用本软件。

瑞星客户服务联系方式

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

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

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

网址: http://www.rising.com.cn

邮政编码: 100190

通信地址:北京市海淀区中关村大街 22 号中科大厦 1408 室

2013 年 8 月 北京 · 中国



重要声明

忠告用户

湍星客户服务联系方式
第一章 软件产品说明 · · · · · · · · · · · · · · · · · · ·
1.1 产品组成 ················1
1.2 应用环境・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1
1.2.1 管理中心 ・・・・・ 1
1.2.2 安全虚拟设备 ・・・・・ 2
1.2.3 日志中心 ······2
1.2.4 升级中心 · · · · · · · · 3
1.2.5 查杀协作 · · · · · · · · · · · · 3
第二章 软件概述······5
2.1 管理中心
2.2 安全虚拟设备・・・・・・・・・・・・・・・・・・・・・・・・・6
2.3 日志中心 6
2.4 升级中心 · · · · · · · · 6
2.5 查杀协作 · · · · · · · · 6
第三章 安装与卸载 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
3.1 安装准备 ······ 7
3.1.1 通信端口 ・・・・・・・・・・・・・・・・・・・・・ 7
3.1.2 产品序列号 •••••• 7
3.1.3 网络连接 ······ 8
3.1.4 数据库 ····· 8
3.1.5 VMware 环境 ······ 8
3.2 组件安装 ······ 9
3.2.1 管理中心
3.2.2 日志中心15
3.2.3 升级中心 •••••••20

3.2.4 查杀协作 •••••••25
3.2.5 安全虚拟设备 •••••••30
3.3 导入 vCenter 终端 ••••••35
3.4 导入授权证书•••••••39
3.5 激活安全虚拟设备 ····································
3.6 分配产品授权42
3.6.1 单独分配 •••••••42
3.6.2 批量分配 •••••••44
3.7 组件卸载 ••••••••46
3.7.1 安全虚拟设备 ••••••••••••••••••••••••••••••••••••
3.7.2 其他组件 •••••••48
第四章 系统管理 ····································
4.1 管理中心
4.1.1 控制台 ••••••52
4.1.2 警报 ••••••53
4.1.3 报告 ••••••54
4.1.4 终端 ••••••55
4.1.5 杀毒 ••••••62
4.1.6 系统 ···································
4.2 安全虚拟设备 •••••••75
4.2.1 系统信息
4.2.2 配置管理网络・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・76
4.2.3 配置密码 ••••••76
4.2.4 重启系统 ••••••••••••••••••••••••••••••••••••
4.2.5 退出系统 •••••••77
4.3 管理工具・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・78
4.3.1 远程安装工具・・・・・・・・・・・・・・・・・・・・・・・・・・78
4.3.2 域脚本安装工具····································

(+

附来一 北京场生信息技术有限公司间介 ····································	• • • • • • • • • • • • • • • • • • • •
叫寻 北古世日传自并少士四八百姓人	0.1
5.2 文件监控・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	••80
5.1 手动查杀・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	••80
第五章 杀毒・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	••80
4.3.3 隔离区管理工具・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	••79

(+

第一章 软件产品说明

1.1 产品组成

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

1. 光盘:包含用户所购买的瑞星虚拟化系统安全软件所有程序。

2.《使用手册》:即本手册,通过阅读它,掌握本软件的详细使用方法和技巧。

3.《客户服务指南》:该指南将帮助用户获取技术支持和服务方面的信息。

4.《快速安装指南》:指导用户快速掌握软件安装的方法。

5. 产品序列号:为本套产品分配的唯一身份证明,缺少它,本软件将无法安装。
 (注意:产品序列号见本手册封二)。

6.《产品组件清单》:用于核对产品组件,以确定产品的完整性。

7.《功能快速查阅表》:了解产品主要功能,帮助用户快速查阅"使用手册"
 中相关功能的详细描述。

 8.《注册扩容指南》:该指南详细介绍了购买本产品后如何进行产品注册和 产品扩容。

1.2 应用环境

1.2.1 管理中心

- a. 软件环境
 - (1) 操作系统

Windows 2003 Server SP2 (32-bit, 64-bit) Windows Server 2008 (32-bit, 64-bit)

Windows Server 2008 R2 (64-bit)

(2) 其它

Web 服务器: IIS 6.0 以上

数据库: MySQL 5.0 以上

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

瑞星虚拟化系统安全软件 1

瑞星虚拟化系统安全软件使用手册发布版_20130830.indd 1

2013/9/16 9:35:27

软件产品说明

b. 硬件和网络要求

CPU: 800MHz 以上

内存: 4GB

硬盘空间: 5GB

网络环境: 100M 以上网络, 需一个固定 IP 地址

1.2.2 安全虚拟设备

- a. 软件环境
 - (1) 操作系统

VMware vCenter 4.0.0 及以上

ESXi 5.0.0, 5.1.0

(2) 其它

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

VMware Endpoint Protection 支持的操作系统: Windows XP SP2 (32-bit) 、Windows 2003 SP2 (32-bit、64-bit) 、Windows Vista (32-bit) 、Windows 7 (32-bit) 、Windows 2008 (32-bit、

64-bit)。(对于最新支持的客户机平台请参考 VMware 文档)

b. 硬件和网络要求

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

支持的 vSwitch: standard vSwitch 标准虚拟机交换机或第三方 vSwitch

虚拟交换机 -- Cisco Nexus 1000v

内存: 2GB, 内存容量需求取决于 SVM 保护的虚拟机数量 硬盘空间: 20GB

1.2.3 日志中心

- a. 软件环境
 - (1) 操作系统

Windows 2000 (32-bit)

建议以下系统:

Windows XP SP2 (32-bit, 64-bit)

Windows 2003 SP2 (32-bit, 64-bit)

Windows Vista (32-bit, 64-bit)

Windows 2008 (32-bit, 64-bit)

Windows2008 R2 (64-bit)

Windows 7 (32-bit, 64-bit)

b. 硬件和网络要求

CPU: 800MHz以上

内存: 512MB 以上

磁盘空间: 1GB 以上

1.2.4 升级中心

a. 软件环境

(1) 操作系统

Windows 2000 (32-bit)

建议以下系统:

Windows XP SP2 (32-bit, 64-bit)

Windows 2003 SP2 (32-bit, 64-bit)

Windows Vista (32-bit, 64-bit)

Windows 2008 (32-bit, 64-bit)

Windows2008 R2 (64-bit)

Windows 7 (32-bit, 64-bit)

b. 硬件和网络要求

CPU: 800MHz以上

内存: 512MB 以上

磁盘空间: 1GB 以上

1.2.5 查杀协作

- a. 软件环境
 - (1) 操作系统

Windows 2000 (32-bit)

建议以下系统:

Windows XP SP2 (32-bit, 64-bit)



Windows 2003 SP2 (32-bit, 64-bit) Windows Vista (32-bit, 64-bit) Windows 2008 (32-bit, 64-bit) Windows 2008 R2 (64-bit) Windows 7 (32-bit, 64-bit)

b. 硬件和网络要求

CPU: 800MHz 以上

内存: 256MB 以上

硬盘空间: 500MB 以上

第二章 软件概述

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

2.1 管理中心

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

安全配置文件

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

管理控制台

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

控制台支持的主要功能包括:

全面的系统日志(警报、事件、扫描记录等)展示与图表分析;

客户虚拟机安全配置与管理;

自定义个性化版面配置;

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

内建安全

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

数字签名用于认证系统组件并验证规则的完整性;

会话加密可保护在组件之间交换信息的机密性。

软件概述

2.2 安全虚拟设备

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

病毒防护

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

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

2.3 日志中心

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

2.4 升级中心

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

2.5 查杀协作

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

第三章 安装与卸载

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

3.1 安装准备

3.1.1 通信端口

瑞星虚拟化系统安全软件需要开放以下默认端口的访问权限: 管理中心

- 管理: 29443
- 通信: 29121
- 其他: 29080

升级中心

● 通信: 29088

日志中心

- 通信: 29086
- MySQL 数据库
- 通信: 3306

3.1.2 产品序列号

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

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

安装与卸载

3.1.3 网络连接

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

3.1.4 数据库

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



图表 3-1

3.1.5 VMware 环境

瑞星虚拟化系统安全软件安全虚拟设备部署需要提供如下 VMware 环境:

VMware vCenter 4.0.0 或以上;

ESXi 5.0.0 或 5.1.0;

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

3.2 组件安装

3.2.1 管理中心

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

自动安装	星序	_ 🗆 🗙
	欢迎使用瑞星软件! 请稍候	
		(E tQ)

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。

<u> 岩星虚拟化系统安全软件</u>	_
星欢迎悠	
欢迎使用瑞星虚拟化系统安全软件安装向导,本向导将正面 化系统安全软件。	崩引导您安装瑞星虚拟
强烈建议您在继续安装之前关闭其它所有正在运行的程序。 能产生的相互冲突。	,以避免安装过程中可
警告:本程序受到版权法及国际条约的保护。	
未经授权复制或散发本程序,或其中的任何部分,都可能会 惩,并将受到法律允许的最大处罚。	会受到民法与刑法的严
单于"了一卡"继续完准,单于"面当"得出完准得度	

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。

🔜 瑞星虚拟化系统安全软件	_ 🗆 🗵
最终用户许可协议 在继续安装之前,请阅读下面的重要信息。	
请任组阅读下面的最终用户许可协议,您必须在继续安装 "PageDora"键阅读协议的其它部分。	之前接受本协议。按
最终用户许可协议	-
重要提示: 在您使用端星软件产品(包括但不限于"瑞星虚拟化系约 "本软件"或"本软件产品")之前,请务必仔细阅读4	安全软件" ,以下称 最终用户许可协议(
以下称"本协议"或"BULA"),任何与本协议有关的到 是按本协议的条款而投权您使用的,同时本协议亦适用于 的后期发行和升级。您在安装本软件产品前应仔细阅读才 任备险动手限到提足公司表在的色表条形 致进口户的权利	件、电子文档等都应 任何有关本软件产品 协议的各项条款,包 限制 你保证,在使
用本软件产品之前,已理解并接受本协议。 1. 本协议是您(自然人、法人或其他组织)与本软件产品的	权利所有人北京瑞星 🚽
, ● 既接受(A)]	○ 我不接受 @)
上一步(1)下一步(1)	

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。

。瑞星虚拟化系统安全软件 定朝安装 请选择需要安装的组件	
典型安装 ✓ 核心组件 ── 常理中心 ── 升級中心 ── 日志中心 ── 互糸协作	▲ 查杀协作 查杀协作是部署在每个客户虚 拟机(GWM)上负责病毒隔 离、查杀后处理的安全组件。
	当前选择 1.22 M
上一步 (2) [下一步	2000 完成 (E) 取消 (C)

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。

择数据库的类型	正在运行的MySQL数据库	-
数据库相关参数		
数据库服务器:	Server	训试连接
端口:	3306	
数据库名称:	rising	
用户名:	root	
審 码:	****	
12 H):	******	

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。

瑞星虚拟化系统安全软件 | 11

2013/9/16 9:35:28

选择数据库的类型	[正在运行的HySQL数]	揺库
数据库相关参数 一 数据库服务器: 端口: 数据库名称: 用户名:	着星度想化系统安全软件	▲
密码:	*****	

图表 3-7

第七步: 在【管理中心选项】界面设定管理中心参数, 点击【下一步】继续安装。

AT. D	管理中心参数 ——		-
6 3	主机名 (<u>1</u>):	193. 168. 12. 8	
27	端口 (https) (L):	29443	
	其它参数		
e In	端口 (http) (h):	29080	
2	端口 (TCP/IP) (§):	29121	
•			

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。

Program File	s\Rising\RVS		浏览(2)
择其它分区:		可用な過かり	66 元 73月 (41)
	5122	979	が高空间(m) 121.705

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。

1942年2011天の大文王で「「 「装信息 安城程序准备完成	
诸确认以下的信息是否正确。如果要修改信息,请单击"上 步"继续。	一步"。单击"下一
当前信息:	
选择目标文件夹 C:Vrogram Files\Rising\RVS 安装的组件列表: 校心组件	*
管理中心	T
•	<u> </u>

图表 3-10

第十步:显示安装过程信息。

3. 瑞星虚拟化系统安全 安装过程中	全软件 東天日期: 2012-20-00 00-14	- O ×
∃#IJAK本・1.0.0.6	3年9月日来的•2013~06~02 06:44	
	备份安装文件	
	消息中心组件 (&vSMSG)]
Ŀ	一步 む 下一步 む 完成 む 取消(Ø

图表 3-11

第十一步:完成瑞星虚拟化系统安全软件管理中心安装过程。

图表 3-12

3.2.2 日志中心

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

自动安装	程序	_0×
	欢迎使用瑞星软件!请稍候	
		j
		i ti chi
	因素 2,12	

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。

瑞星虚拟化系统安全软件	
<u> 着星欢迎悠</u>	
欢迎使用瑞星虚拟化系统安全软件安装向导,本向导将正确引导缆 化系统安全软件。	悠安裝瑞星虚拟
强烈建议您在继续安装之前关闭其它所有正在运行的程序,以避约 能产生的相互冲突。	电安装过程中可
警告:本程序受到版权法及国际条约的保护。	
未经授权复制或散发本程序,或其中的任何部分,都可能会受到限 惩,并将受到法律允许的最大处罚。	民法与刑法的严
单击"下一步"继续安装,单击"取消"退出安装程序。	
上一步迎【下一步观】 完成即	取消C)

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。

诺星虚拟化系统安全软件	<u> </u>
最终用户许可物议 在继续安装之前,请阅读下面的重要信息。	-
请仔细阅读下面的是终用户许可协议,您必须在继续安装之前接受本协议。按 "PageDown"键阅读协议的其它部分。	
最终用户许可协议	1
重要提示: 在您使用瑞星软件产品(包括但不限于"瑞星虚拟化系统安全软件",以下称 "本较性"。雷···大致性产品")之命,该发动好细丽读术是终田口没可知()/	
以下称"本协议"或"EULA"),任何与本协议有关的软件、电子文档等都应 是按本协议的条款而授权您使用的,同时本协议亦适用于任何有关本软件产品 的后期发行和升级。签在安美本软件产品前应仔细阅读本协议的各项条款,包	
括免除或者限制编星公司责任的免责条款及对用户的权利限制。您保证,在使用本软件产品之前,已理解并接受本协议。 1	
本物改差怒(目然人、法人或具他组织)与本软件产品的权利所有人北京瑞星 () 野葉等(面) () サズ接巻(面)	-
上一步(2)下一步(2)完成(2)取消(

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。

] 瑞星度携化系统安全软件 定制安装 请选择需要安装的组件	
典型安装 ▼ 核心组件 	日志中心 日志中心是系统运行过程中产 生的报警、错误、信息日志、 看升日志、講案日志等的收集 管理器,通过部署多个日志中 心可实现日志上指的负载均 衡-
	当前选择 0.94 M
上─步® (下── ─ ─────────────────────────────────	完成 (2) 取消 (2)

图表 3-16



 二日本

 第二日本

 <

第五步: 在【客户端选项】界面设定客户端参数, 点击【下一步】继续安装。

图表 3-17

第六步:在【日志中心选项】界面设定日志中心参数,并配置数据库信息。

	□ 日志中心参数 — 端口 (g):	29086	
	数据库信息 数据库服务器:	Sarvar	
Th	端口:	3306	
SYN	数据库名称:	rising	
	用户名:	root	
•	密 码:	****	_

提示:数据库配置需与管理中心保持一致。

日志中心参数	
数i 第星度机化系统安全软件 X 数: 端	<u>测试 (1)</u>
数: 用, 密码: #******	

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。

\Program Files\Rising\RVS 选择其它分区: <u>计区 分区大小 00) 可用空间 00) 所需空</u> : 5122 978 10				•	医马利平 化叶文派
<u>⊠ 分区大小 00) 可用空间 00) 所需空</u> : 5122 978 10	E (B)	浏览(ising\RVS	\Program Files\] b择其它分区:
	<u>創 (M)</u> 05.169	所需空间 105.	可用空间 (M) 978	分区大小 (M) 5122	

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。

1. 瑞星虚拟化系统	充安全软件					_ 🗆 🗵
安装信息 安装程序准备完	咸					23(0)
请确认以下的信 步"继续。	息是否正确。	如果要修改信息	,请单击	"上一步",	• 单击"	₩
当前信息:						
选择目标文件 C:\F 安装的组件列 核心 日志	夹 Yrogram Files' 表: 组件 中心	\Rising\RVS				A
T						₹ 1
	上一步创	下-步00		完成①]取消	

图表 3-21

第十步:显示安装过程信息。

衰过在中 当前版本:1.0.0.8	更新日期:2013-08-02 08:44	
		2
备份安装文	5件	
消息中心组	1件 (RVSMSG)	
1.15.25	[TTO NUL CON

图表 3-22

瑞星虚拟化系统安全软件已经成功安装到您的电脑中。 11日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	
27 秒钟后窗口格关闭	
上一步也」下一步如 完成① 取消	₿©

第十一步:完成瑞星虚拟化系统安全软件日志中心安装过程。

图表 3-23

3.2.3 升级中心

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

自动安装	程序	×
	欢迎使用瑞星软件!请稍候	
		j
		it tu

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。

崙星虚拟化系统安全软件	
星欢迎您	
欢迎使用瑞星虚拟化系统安全软件安装向导,本向导将正确引导悠安装现 化系统安全软件。	星虚拟
强烈建议您在继续安装之前关闭其它所有正在运行的程序,以避免安装远 能产生的相互冲突。	提中可
警告:本程序受到版权法及国际条约的保护。	
未经授权复制或散发本程序,或其中的任何部分,都可能会受到民法与刑 惩,并将受到法律允许的最大处罚。	以法的严
单击 "下一步"继续安装,单击"取消"退出安装程序。	
上一步 化 下一步 化 完成 化 1	取消 ©)

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。

🖳 瑞星虚拟化系统安全软件	_ 🗆 🗵
最终用户许可协议 在继续安装之前,请阅读下面的重要信息。	20
请仔细阅读下面的最终用户许可协议,您必须在继续安装之前接受本协议。 "PageDown"键阅读协议的其它部分。	ġ.
最终用户许可协议	-
重要提示: 在悠使用瑞星软件产品(包括但不限于"璃星虚拟化系线安全软件",以下? "本软件"或"本软件产品")之前,请多必仔细阅读本最终用户许可协议 以下称"本协议"或"zuLa"),任何与本协议有关的软件、电子文档等都引 是按本协议的条款而授权您使用的,同时本协议亦适用于任何有关本软件产, 的后期发行和开纸。您在安装本软件产品简应任细阅读本协议的各项条款。?	你 (立品 包
指免除較著機制視量公司责任的免责条款及对用户的权利限制。您保证,在 用本软件产品之前,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)与本软件产品的权利所有人北京場。	e I
○ <u>既接受()</u> ○ 我不接受(0)	
上一步 (2) 下一步 (2) 完成 (2) 取消	i©

图表 3-26

5 端星虚拟化系统安全软件 定制安装 请选择需要安装的组件	
典型安装 ★型安装 ● ダブン 核心组件 ● ヴ理中心 ● ジブン が成中心 ● 日志中心 ● 雪茶物作	▶ 升级中心 升级中心通过http协议向系统 其它组件提供升级服务,通过 部署多个升级中心可实现升级 的负载均衡。
	当前选择 1.30 M
上一步 CD 下-	- 步 (2) 完成 (2) 取消 (2)

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

图表 3-27

第五步:在【客户端选项】界面设定客户端参数,点击【下一步】继续安装。



图表 3-28



第六步:在【升级中心选项】界面设定升级中心参数,点击【下一步】继续安装。

设定升级中心参数		-3
(F.)	「升级中心参数	
	端口(2): 29088	
		d
12/1		

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。

^技瑞星 软件到目	录:		
Program Fil 译其它分区:	es\Rising\RVS		浏览(2)
X	分区大小 (M) 5122	可用空间 (M) 1007	所需空间 (M) 105.996

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。

5. 端星虚拟化系统安全软件 安装信息 安装程序准备完成	×
请确认以下的信息是否正确。如果要修改信息, 步"继续。	请单击"上一步"。单击"下一
当前信息: 选择目标文件夹 C:\Yrogram Files\Rising\RVS 安装的组件列表: 核心组件 升级中心	<u>*</u>
ब	T T
Ŀ─₽₽	完成① 取消 ②

图表 3-31

第九步:显示安装过程信息。

国 瑞星虚拟化系统安全	全软件	<u> ×</u>
安装过程中 当前版本:1.0.0.8	更新日期:2013-08-02 08:44	20
	备份安装文件 消息中心组件 (&vsmsg)	
Ŀ	一步 22 下一步 32 完成 22 取消	©

图表 3-32



□ 瑞星虚拟化系统安全软件	<u>- ×</u>
治 来	
場量虚拟化系统安全软件已经成功安装到您的电脑中。 場合の目的では、 場合の目的では、 場合の目的では、 場合の目的では、 場合の目的では、 場合の目的では、 していたいでいでいたいでいたいでいでいたいでいでいでいでいたいでいでいでいでいたいでいでいでいでいたいで	
27 秒钟后窗口将关闭	
上一步(12)下一步(12) 一元成(12) 取消(1	0

第十步:完成瑞星虚拟化系统安全软件升级中心安装过程。

图表 3-33

3.2.4 **查杀协作**

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

自动安装	程序	_0×
	欢迎使用瑞星软件!请稍候	
		ſ
		(LE LEQU)

图表 3-34

安装与卸载

如連律用端星虚拟化系统安全软件安装向导,本向导将正确引导您安装端。 化系统安全软件。 副2建议您在继续安装之前关闭其它所有正在运行的程序,以避免安装过。 2产生的相互冲突。 2音:本程序受到版权法及国际条约的保护。	悠安装瑞星虚排 免安装过程中可
融建议您在继续安装之前关闭其它所有正在运行的程序,以避免安装过; 2产生的相互冲突。 8告:本程序受到版权法及国际条约的保护。	免安装过程中可
音:本程序受到版权法及国际条约的保护。	
长经授权复制或散发本程序,或其中的任何部分,都可能会受到民法与刑 E,并将受到法律允许的最大处罚。	民法与刑法的严
单击"下一步"继续安装,单击"取消"退出安装程序。	

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

图表 3-35

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

每百些机械来获安全软件 终用户许可协议 在继续安装之前,请阅读下面的	重要信息。		
请仔细阅读下面的最终用户许可 "PageDown"键阅读协议的其它部	协议,您必须在錮 分。	建续安装之前接受本协议。按	ŧ
最终用户许可协议			4
重要提示: 在您使用瑞星软件产品(包括低 "本软件"或"本软件产品") 以下称"本协议"或"EVIA")	不限于"瑞星虚排 之前,诸务必仔细 ,任何与本协议不	机化系统安全软件",以下和 阳阅读本最终用户许可协议(有关的软件、电子文档等都应	R
是按本协议的条款而授权您使用 的后期发行和升级。您在安装本 括免除或者限制端星公司责任的 用本软件产品之前,已理解并接	l的,同时本协议》 软件产品前应仔约 免责条款及对用F 授本协议。	が适用于任何有关本软件产品 11阅读本协议的各项条款,包 2的权利限制。您保证,在包	
1. 范围 本协议是您(自然人、法人或其	(他组织)与本软件	中产品的权利所有人北京瑞县	
6	我接受(A)	C 我不接受 (D)	

图表 3-36



3. 瑞星度視化系统安全软件 定制安装 谱选择需要安装的组件	>
<u>典型安装</u> 	▼ 査杀协作 査杀协作是部署在每个客户虚 损机(cwp)上负责病毒属 黨、查杀后处理的安全组件。
	当前选择 1.22 #
上一步 (2)	步迎 完成 12) 取消 12)

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

图表 3-37

第五步:在【客户端选项】界面设定客户端参数,点击【下一步】继续安装。

3. 瑞星度拟化系统委 客户端选项 设定客户端参数	安全软件	
	管理中心参数 主机名 ①: [193.166.12.8 端口0attps)① [29443	<u> </u>
	上—步 C) 下—步 C) 🦩	記成 (2) 取消 (2)

图表 3-38

\Program File	s\Rising\RVS		浏览(2)
选择其它分区: 分区	分区大小(M)	可用空间 (11)	所需空间(11)
:	5122	1006	101.862

击【下一步】继续安装。

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

图表 3-39

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

瑞星虚拟化系统安全软件	_ 🗆 >
装信息 安峽程序准备完成	
唐确认以下的信息是否正确。如果要修改信息,请单击"上一步 步"继续。	"。单击"下一
当前信息:	
选择目标文件夹 C:\frogram Files\Rising\RVS 安装的组件为表: 核心组件 查杀协作	A
4	₹ ₹
上ー步 (2) (下 一步 (2) 完成 (2)	取消 (C)
图表 3-40	

第八步:显示安装过程信息。

马瑞星虚拟化系统安全 安装过程中	全软件	
当前版本:1.0.0.8	更新日期:2013-08-02 08:44	-30
	备份 安装 文件	
	消息中心组件 (RVSMSG)	
		-
Ň		
Ŀ	步 E 下步 E 完成 E 取消	0

图表 3-41

第九步:完成瑞星虚拟化系统安全软件查杀协作安装过程。



图表 3-42

3.2.5 安全虚拟设备

NUT (C)	M EXCORA	· 22 (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	
部署 017 模板 (1)	8 m D	- AND	_
28 Q	, , , , , , , , , , , , , , , , , , , ,		
368 (L)	• a20035P2_X64_20.171		
(通知 NA Marketplace(2)	(1) 数据 按规则数 性能 社会中举件 整括 拉利台 初期	Half Printing valued	
打印映射(2)	, Lá Babeller	天國國現卡 王	
建合金	T 2, 2 di Met I		
() mes.ska () Text.sky.De	与物理机一样。虚拟机是运行操作系统和应用程序的软件计算机。虚拟机上安装的操作系统和为客户机操作系统。	12 HI 31	
() engine_comp	因为時台虚熱机是陽面的计算环境。所以思可以将虚鬆机用 化調査(ため环境部)が対象。原用来整合服を設立用容	a set and a set	
D Rshp-S/M	序.	878 Q	
(D Rang-SWM-d	在 vCenter Server 中,虚拟机在主机或解集上运行。同一		
6) SM_04	台主机可运行多个虚拟机。		
C) SIM_05		ISE A	
G test_inittab	****		
(E 🕘 1Mware_vCenter	量奉社穷	A DECEMBER OF THE OWNER OWNER OF THE OWNER OWNE	
B Mindows_Clerits	目 关闭虚拟机	Scenter Server	
(j) WIN2003SP2,	10 挂起齿风机	vSohern Client	
(B Wh2000064	D. 1018-0-1010-2578		
(j), WIN7(32bRs)	O MARTINGLICE		
(B) WHOP(32045		788648	
		J mgc SP max	
E#		名称. 目標 家伙古包含: •	- 189
		THOTAGE - TROAT	-

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

图表 3-43

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

27 部署 OVF 模板 22 选择源位置。			-0>
 2007 援気が知信息 金谷和白江雪 金谷和白江雪 田 主初(群集 渋渡池 総型格式 	从文件或 LRL 部署		
風性 即将完成	输入一个 URL 以从 Internet 下载和安	· · · · · · · · · · · · · · · · · · ·	1008 10可从您的
帮助(日)		≤上一步	下一步 ≥ 取消

图表 3-44
戸部署 OVF 模板			_	
OVF 极板详细信息 验证 OVF 极极详细信息				
選 2017 或27m(加急 最終用) 中述可协议 名称的位置 3 主抗保持系 劳活线系 整合称式 属性 即将完成	产品: 黄本: 供度离: 发布若: 下載大小: 占用空词: 撇達:	Rising-SWI 1.1.5-baid+5530 Rising Inc 证书不存在 282.8 MB 302.1 Mg (精制要备) 1.6.0 GB (度量备) Rising Security Virtual Machine		
帮助(出)				y

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

图表 3-45

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

□部署 0¥7 模板		Þ
最终用户许可协议 接受最终用户许可协议。		
選 CMF現版計畫直直 量代用户许可协议 名称可应量 图 生机移用 强造油 塑造作式 属性 即将完成	■ ■ ■ ■ ■ ■ ■ ■ ■ ■	
帮助(日)	≤上一步 下一步 取消	

图表 3-46

瑞星虚拟化系统安全软件 | 31

一步】继续部署。

sing-SWM 称量多可包含 80 个字符, J 单位置: 2 [2] VCenter_12.21 10 [1] [Esso5.]	并且在清单文件夹中 <i>。</i>	必须是唯一的。	
株量多可包含 80 个学符 , 引 単位置: - [2] vCenter_12.21 - 0 ■ E5555.1	中且在清单文件夹中级	609. 2 *t—69.	
Essis.1			

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

图表 3-47

第六步:在【主机/群集】界面选择部署安全虚拟设备模板的主机或群集,

点击【下一步】继续部署。

○ 20 20 00 20 20 20 20 20 20 20 20 20 20	i容易的模核? 3	
帮助(日)	<u>≤</u> #-٦	取消

图表 3-48

团部署 OVF 模板	
资通油 选择资源池。	
28 20年現板浮銅道皇 星校用户许可协议 名称30位章 主机成在集 资源地 词虚构成 问道说明射 属性 即将完成	法操作要在其中審尋狀模板的资源油。 资源油允许在主机或群集的实行计算资源的分层管理。虚拟机和子油共享其尖油的资源。 □ Ⅰ 193.168.12.20 ● Linux_Clents ● STM ● Vinves_Vinder_Server ● Vinves_Vinder_Janager ● Windows_Clents
#Bh(H)	<hr/> <hr< td=""></hr<>

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

图表 3-49

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

部署 OVF 模板				- 0
磁盘格式 想要以什么格式存储。	虚拟磁盘?			
渡 OVF 模板详细信息 最终用户许可协议 名称和位置	数据存储: 可用空间 (GB):	1220G 837.7		
土包// 註葉 透透: 通 金格式 网络映射 犀性 即将完成	C 厚置备延迟置零 C 厚置备置零 C [Thin Provision]			
帮助(出)			≤⊥−₩	取消

图表 3-50

【板洋銅信息 目中洋可协议	裕此 OVF 模板中使用的网络映射到悠清单的网络中						
1位置	源网络	目标网络					
<u> 詳集</u>	VM Network	VM Network					
R i							
	描述:						
	The VM Network network						
	,						

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

图表 3-51

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

	-	
5 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5	阿格記登 主机名 Distrg-SVM 防病事業電管理中心(PMC,例如:https://192.168.10.100.29443) PMCP自动表取IP	
	IP場값 193、166、12、225 子内純印 255、255、255、0 致以得关 193、166、12、2	
	首述0>>服务器 ◎ . 8 . 8 . 8	

图表 3-52

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

F 櫃板详细信息 终用户许可协议	单击"完成"时将后 部署设置:	3动部署任务。	
称和位置	OVF 文件:	D:\Rising-SVM.ova	
<u>01081980</u> 30834	下载大小:	282.8 MB	
<u>象格式</u>	占用空间:	302.1 MB	
缩映射	名称:	Rising-SVM	
性	文件夹:	Esxi5.1	
格完成	主机/群集:	193.168.20.20	
	资源泡:	SVM	
	数据存储:	1220G	
	磁盘置备:	Thin Provision	
	网络映射:	"VM Network"到"VM Network"	
	网络映射:	"vmservice-vshield-pg"到"vmservice-vshield-pg"	
	IP 分配:	固定的, IPv4	
	原性:	hostname = Rising-SVM	
	康性 :	pmc_url = https://193.168.12.8:29443	
	康性 :	dhcp = False	
	属性 :	ip = 193.168.20.225	
	属性:	netmask = 255.255.255.0	
	属性 :	gateway = 193.168.12.2	
	4		

图表 3-53

3.3 导入 vCenter 终端

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

D 22	× 💼
← → C	🕼 þærð://193.168.12.8:29443/rvsmc/Home/Login?from=%2frvsmc%2fEp%3fgroupGuid%3d#includeChildren=true#pr🏠 🚦
Margaret.	
	4976
	Rising vin System Security Software
	III PA admin
	974
	포고
	STATUT AND ADDRESS ADDRESS TO ADDRE
100000000000000000000000000000000000000	原作所有もの口子出現構成的自我本有限公司

图表 3-54

- → C (2) (24) (25) (7)	193.168.12.8:29443/rvrmc/Hone/Hone	<u>ث</u>
瑞星虚拟化系统安全软件	411 拉制台 240时期图 ▼	
11 控制台 ● 警察	Statistic : 所有好機 ··· Red Frage ·· Red Frage ·· ·· Red Frage ·· ·· Red Frage ·· ·	
 一 県告 二 県 谷魂 〇 川 谷魂 〇 介 永道 〇 介 永道 ○ 介 永道 ○ 介 永道 ○ 介 永成 日志 	WTRACLER 国際部には他的人:0 世好は:1 単行物には、他的人:0 世好は:1 単行物に、 9000000000000000000000000000000000000	● 新版严重性 ● 著音 ● 错误
日志用户角色	我的第户状态 22 杂曲终端最新记录	
策略俱板 任务 计划任务 授权证书 设置	用PS: 2, 40min 10000月15日1748: 発色: Administrators 上が建築: 231707110225 上が建築: 231707110225 上が建築: 3170711025 上が建築: 3170711025 上が建築: 3170711025 101712 10172 101712 10172 101712 1017 1017 1017 1017 1017 1017 1017 1017 1017 1017 1017 1017 1017 1017 1	Pjilij
	(messade) 201 (STELN)	
	1	

第二步:显示瑞星虚拟化系统安全软件管理控制台主界面。

图表 3-55

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

315106 计器层		终端	包含于组	• UD&f.	: BAU -					
	技术:		9 .SI	6:©P A	鼠 : 不限		*			
1 12时日 ● 警报	國导入终	端(vCenter)	O stitlin	▶ ₊ 83080		会 立即	на 🧠 н	12.2 m	01.50 B	括权分配
		名称		IP		織口	肉型		操作系统	E
·····································		ISERS		193.168.12	.8 2	9010	物理机	-		-
宁杀西										
查杀日志										
MAKE O 144										
Ba										
用户										
角色										
用电线仪 任务										
计划任务										
授款证书										
τ.π.										
						_		-		

图表 3-56

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

← → C 登址成://193.168 司SING I開催 市田市市// 系統在全教社	.12.8:29443/rvenc/Ep/Ep?group5uid=≉includeChild	dren=true&pageIndex=1&pageSize=100 😚
21	:: 从vCenter获取终端信息	22
· TRAB	·····································	· · · · · · · · · · · · · · · · · · ·
	服务器地址:	操作系统 E890
	服务器端口:示例:443	-
查杀日志 延来[7	用户名: 请航入用户名	
E C Str	老時 : 通输入密码	
用户	道写vShield 管理中心信息	
用臣 策略褒极	服务器地址: 示例:192.168.13.35	
任务 计划任务	服务器端口: 示例:443	
抵积证书	用户名: 油输入用户名	
	宏码: 语输入密码	
	共1条记录 1/1	下一歩 取消 1 4 1 一 1 1 下一 平 新賀星示 100 * 条

图表 3-57

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

_ ##### ×		- @ X
← → C Butter://19 → C Butter://19 → HUNC HARE	3.168.12.8:29443/rvsmc/Ep/Ep?groupGuld=#includeChildren=tru	e&pageIndex=l&pageSize=100 🖓
 第目目記(な系統支全状件 第日 第日<!--</th--><th></th><th>22 34, 79,256 35, 92092 36, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72</th>		22 34, 79,256 35, 92092 36, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72
21.0892	共1条记录 1/1 <u>4 上</u>	-页 1 〒-页▶ 4次2示 100 ★ 条

图表 3-58

31510 3端层 端星虚拟化系统安全软件		冬端 包含		ROGE: 1					
	投票:		● 2R C	₽ 类型:	不職	*			
. with	國导入终期的	Center)	see A	- 移动到 6) #R# 合立	即升级 《开始》	·····································	图 预权分配	
会 我肯	8	名称	-	IP	魏口	类型	操作系统	and a second	ESX
□		RS		193.168.12.8	29010	物理机	-	-	
日本語									
□ 丁· 赤● 査杀日志									
MARIZ									
e an									
日志									
用户									
策略模板									
任务									
计划任务									
授权证书									
花童									
							握示		
					共1条记录 1/1	4 上一页 1	Υ-Π ►	导入vCenter操作	成功

第六步:确定导入后,右下角弹出窗口提示:导入 vCenter 操作成功。

图表 3-59

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

31510 计编号 · · · · · · · · · · · · · · · · · · ·	L	终端		• NBQ:				
	22.5	R :	* S	\$\$ © ₽ 555	: 不限	*		
(1) 1240 B	1	导入终端(vCente	er) 🗘 🖏 🖏 🖓	A4 883393		立即开闭 🗍 🔍 :	开始杀毒 🛛 🕵 停止杀毒 📄	3 KR9R
☆ 採告	8	3	缩 -	IP	第日	英型	操作系统	ESX
□ 副 终端	۵	193.169.1	2 222	-	0	成拟主机	VMware ESXi 5.0.0 build-	6
@ 和余祖		D-Win7SP	1-32(12回	-	0	成损机	-	193.168.12
」 今 永高 査糸日志		D-Win7SP	1-64 (122	-	0	虚拟机	-	193.168.12
隔底区 ◎ 系統	2	Dir-Winse		-	0	虚拟机	-	193.168.12
日志		@ Unux		-	0	虚拟机	-	193.168.12
角色		D PMC-12.7	2 Crising-4b	193.168.12.72	0	虚拟机	Microsoft Windows Serve	r 193.168.12
策略模板 任务		Rising-SVI	M-12.73(R	193.168.12.73	0	虚拟机	其他 2.6 x Linux (64 位)	193.168.12
计划任务	۲	@ <u>vCenterSe</u>	rver-12.70	193.168.12.70	0	虚拟机	Microsoft Windows Serve	ır 193.168.12
設置	۲	@ <u>m-2008-8</u>	54	-	0	虚拟机	-	193.168.12
	۲	@ <u>vm-win7-3</u>	2	-	0	虚拟机	-	193.168.12
		-			共19条记录	1/1 4上一页	1 下一页 ▶ 每页显示	100 🔻 🛠

图表 3-60



3.4 导入授权证书

第一步:点击控制台目录下的【系统】/【授权证书】,显示授权证书页面。

Sing Hiller				
星虚拟化系统安全软件	授权证书			
1241 B	日本人授权			
<u>۲۵۵ کی</u>	<u>74</u>	景教评问号	有效自則	ROURE
◎ 报告				
·····································				
11 월8 vCenter(193.168.12.				
<u>-</u> 茶田市				
國家区				
● 系統				
日志				
用户				
用色				
44				
计划任务				
授权证书				
设置				

图表 3-61

 Image: Image:

第二步:点击【导入授权】,输入基本号、选择文件证书导入后【确定】。

图表 3-62



第三步:确定导入授权后,在【授权证书】页面显示授权许可的详细信息。

图表 3-63

3.5 激活安全虚拟设备

·····································	L	终端		- 1 16 BD (R.)C =					
	税	*:	® 81	tk © IP , ⇔M	: 不限	¥			
● 警报	1	导入终端(vCenter)	0 1624	Ap. 移动到	O HR ♦ 3	200升级 🔍 🔍	开始杀毒 🔍	停止杀毒	4 授权分配
前	0	名称		IP	第日	英型	1	制作系统	ESX
□ III K4集 III III vCenter(193.168.12.)	8	193.168.12.22	12	-	0	虚拟主机	VMware ES	ixi 5.0.0 build-6	in e
G Dieli	8	D-Win7SP1-3	2《12图		0	虚拟机	-		193.168.12
至头日空 四 - 7- 3- 18	8	D-Win7SP1-6	4(12四	-	0	1915101	-		193.168.12
帰軍区 日 😡 系統	8	Din-Win98			0	1515140	-		193.168.12
- 日志 用の	8	Dinus		-	0	1511121			193.168.12
70/~ 角色	8	B PHC-12.72 (r	ising-4b	193.168.12.72	29010	虚拟机	Microsoft V	Vindows Server	193.168.12
策略模板 任务	8	B Rising-SVM-1	2.73	193.168.12.73	5557	安全虚拟设备			193.168.12
计划任务	8	B vCenterServer	12.70	193.168.12.70	0	虚据机	Microsoft	Vindows Server	193.168.12
ixeourn 设置	8	D ym-2008-64		-	0	虚据机	-		193.168.12
	23	D vm-win7-32		-	0	透訊机	-		193.168.12
		-			共19条记录 1/	4上四菜	1 下一页 Þ	# 7237	100 - 承

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

图表 3-64

第二步:点击安全虚拟设备,显示其激活状态。

□ 终端管理	× 1 約線信息	× 🔳	- 6 ×
← ⇒ C () but	ps://193.168.12.8:294	43/rvsac/Ep/EpDetail?ep=423b6fdd-0a6f-c7fd-f4ed-f8e0f4becf73	\$
终端:Rising-S	VM-12.73		
 □ 評論准直 ● 要点 今 用面白名串 □ Q 系统 □ Q 系统 ① R ① H ① H ① H ① H ① H ○ 所 ○ 用 ○ 日 ○ □ ○ □	→ 正线	19編5版: Photop 574-1273 典型: 学生成的合称 新聞編: Resolitiong in - Center(193168.1270-443) + Datacenter + vm + FV Phot: 193168.1273 編ロ: 9987 資産業: 1.5.8 単位: :	5 Test अन
		vShield:193.168.12.71 状态:未潮语	赵康
	授权状态	が編正統: 193.168.12.222 主元CPU: 2 个 赤篇: ○己成权 ●未成权	執定
-1			

图表 3-65

第三步:点击【激活】按钮,确定激活安全虚拟设备。

6 终端管理	×) 凸 终端信息	×	- 6
← ⇒ C Bb	.//193.168.12.8:294	43/rvsmc/Bp/BpDetail?ep=423b6fdd-0a6f-c7fd-f4ed-f8e0f4becf73	☆
 Hmaa Ba Malss Ks Ks Hs Ha Ha 	a et	Higgs: hosp 004-127 Higgs: hosp 004-127 Migg: hosp 004-127 <td< td=""><td></td></td<>	
	授权状态	周電主語: 193.169.12.222 主要にGPU: 2 个 永憲: C ビがR 参考授祝	

图表 3-66



6 终端管理	× /] 终端信息	×	- @ ×
⊢ → C Bbee	p\$://193.168.12.8:294	43/rvsac/Ep/EpDetail?ep=423b6fdd=0a6f=c7fd=f4	ed-f8e0f4becf73
终端: Rising-S	VM-12.73		
 ● 折除恒直 ● 新市 ↑ 用着日5章 ● 系約 日回 日回 任务 并() 	α.e. 268	94歳名称: 用xing-294-12.73 用品: 宇治道(KG)各 所編道: 宇治道(KG)名 用211: 583-584.72.73 編(L): 5857 第代末後: 月後 月年末: 1.8 <u>2011年6</u> 名称: 1.9 	Dataseter - vm - RVS Test
	- B R U S	所国王統:193.16612.222 主統CPU: 2个 計画:の記録訳 ●未続訳	61.66 23

第四步: 激活完成后, 右下角弹出窗口提示: 激活成功。

图表 3-67

3.6 分配产品授权

3.6.1 单独分配

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

1 终端管理	× 门 终端信息	×	
< → C & bu	ps://193.168.12.8:294	43/rvsac/Ep/EpDetail?ep=423b6fdd=0a6f=c7fd=f4ed=f8e0f4becf7	ঃ 🔝
终端: Rising-S	VM-12.73		
● 警报 ● 警报 今 病毒自名单 ● 承兆 日志 任务 升値	Ŧ.K	料確応第: FRang-OM-1273 両型: 宇定道明设备 所確型: FRacEdRight For State(193.16512/0443) + Oktacenter + vm + P18社は: 193.1641272 展記: 5957 酸化素伝: ホルロ 最初:: 1.1.0 <u>ご問任成</u> 最初::	RVS Test 0.77
	激活状态	v6NeHd: 193.168.12.71 读句: 未發展	814
	一接校状态	M国王政: 19316812.222 王政にPU: 2 ↑ 赤国: ○己成权 ※未知政	
41			- 1

图表 3-68

提示:只能为开启状态的安全虚拟设备分配授权。

第二步:选择杀毒【已授权】,点击【确定】按钮,分配杀毒产品授权。

1 终端管理	× □ 终端信息	×	- 6 ×
< → C B but ps	//198.168.12.8:294	443/xvsmc/Ep/EpDetail?ep=423b6fdd=0a6f=c7fd=f4ed=f8e0f4becf73	☆ :
终端: Rising-SVM	1-12.73		
 ● 警察 ● 警察 ← 消機自名率 ○ 承 系统 日志 任务 升頃 	ũ tế	NG&5時: Picrop-SPA-1273 周期: 学会通知记号 外間間: Piccal和记号 Pittable: 1031061273 第61: 5557 BMT25KT: 未有 原形: 1.1.0 <u>気間引点</u> 単位:	rs Test 傑花
	融活状态		
		vShiald: 193.168.12.71 代表:已建始通	简纯改活
	RRUS		
		所難変現: 192160.12.222 変現CPU: 2 个 永喜:幸已読衣 ◎未成衣	國史
1			1

图表 3-69

提示:安全虚拟设备占用的授权计数为其所属物理主机的 CPU 个数。

终端: Rising-SVN	-12.73		
 ※新: Rising-SVM-12 第第第 今月期台店# 回 (2) 末後 日志 住赤 光所 	τu tu	料理(2)(1): FR13(10,0-50%4-12.73 内部: 安定道(14)(3)(2) 所提注: FR12(14)(3)(3)(3)(3)(2)(2)(4)(3) + Da 所提注: FR13(16)(5)(2)(2) 時に3(4): 安加 前に: 50(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(dsender + vm + RVB Test
	古井延逝	vGhinds: 193.168.1271 快志: 世始56	建铸造活
	授权状态	所編主戒: 193168.12.222 主政CPU: 2 个 永道: ※ 乙類保 ◎未期保	an Teresto

第三步:授权分配完成后,右下角弹出窗口提示:授权设置成功。

图表 3-70

安装与卸载

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

3.6.2 批量分配

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

副SING 新編編 新星虚拟化系统安全软件				• I KERK:	ಕಾಣ 🗕						
	浆	*:	* Sf	k © IP ⇔ <u>8</u>	不限	¥					
·····································	ø	导入终端(+Center)	新建组	Þ.4. 8530351 €	388 全立	юна 🛛 🔍 я	给杀毒	第 4 停止杀毒	B 2	(初分記)	
● 报告	0	名称		IP	第日	装置		操作系统		E	S20
의 내 終端 田 ⊮□ vCenter(193.168.12.)	6	193.168.12.222		-	0	成报主机	Vites	ire ESXi 5.0.0 bui	ld-6	-	
🗇 Dietit	8	D-Win7SP1-32 (12	<u>19</u>		0	1215141				193.168	12.2
1 千 永衡 査糸日志		D-Win7SP1-64 (12	Ø	-	0	1515120				193.168	12.2
「編室区 「金 系統	8	Din-Winte		-	0	透照机	-			193.168	12.2
日志	6			-	0	虚招和	-			193.168	12.2
角色	8	PMC-12.72 (rising	40	193.168.12.72	29010	虚据机	Micro	soft Windows Se	wer	193.168	12.2
策略模板 任务	8	Rising-SVM-12.73		193.168.12.73	5557	安全虚拟设备	-			193.168.	12.2
计划任务		D vCenterServer-12.7	2	193.168.12.70	0	虚报机	Micro	soft Windows Ser	ver	193.168	12.2
设置	8	D 10-2008-64		-	0	SIRR.				193.168.	12.2
		@ <u>vm-win7-32</u>		-	0	虚报机				193.168.	12.2

图表 3-71

第二步:点击工具栏【授权分配】按钮,显示授权分配窗口。

17116	股票:	_®38®₽ ≠	12: 不限	•		
WTR	窗与入标编(rCenter) O	新建版 14. 移动物	○ HPR 合立	17升级 《 开始杀毒	泉 停止杀毒 🛛	我权分配
● 括常 ■ 57 M	授权分配				N IS N	ESXI
D 10 vCenter(193.168.12.					6.0.0 build-6.	
C 1981	共选择1台将编进行分	能投权操作 :				193.168.12.3
Ŷ.茶香	名称	ESX0	CPU	是否分配授权		10216912
显示口也 開度区	Rising-SVM-12.73	193.168.12.222	2	■ 授权分配		
9 X 15						193.168.12
日志						193.168.12
角色					ndows Server .	. 193.168.12
策略模板						
任务						193.108.12.
新政定的					ndows Server.	. 193.168.12.3
20				完成 1	8.99	193.168.12
	m mwin7.32		0	1910 H		19316812
	and the second s					

图表 3-72



第三步:为安全虚拟设备勾选【授权分配】,点击【完成】,分配杀毒产品授权。

图表 3-73

第四步:授权分配完成后,右下角弹出窗口提示:所选终端分配授权成功!。

🛞 RISING SHARE 明星虚拟化系统安全软件		_ t	544	包含子組	▼ 礼田4天:	इस्ता 🗢					
10 maio	撩	æ:		* 3	18 O IP #5	2: 不限		*			
 型 元約日 ● 警报 	ø	导入终端的	Center)	O Riszisi	▶ ₄ , 核动面	O HFR	會 立即	Hat Q	开始杀害	第4 停止派遣	5 授权分配
			名称	*	IP			类型		操作系统	ESIG
□ = 944 □ = 944	۵	I 192.	68.12.222		-	0		虚极主机	VMm	are ESX 5.0.0 build-l	s
@ 和余级	B	@ <u>D-W</u>	n7SP1-32	(12F	-	0		虚颜机			193.168.12.3
3 小 永海 査永日志	10	@ D-WA	n7SP1-64	(12月	-	0		虚积机	-		193.168.12.3
「現実区		@ Lin-Y	6n98		-	0		虚积机	-		193.168.12.2
Bā	10	D Line			-	0		虚照机	-		193.168.12.2
用戶 角色	E	D PHC	12.72 C ris	ine-4b	193.168.12.72	290	10	虚积机	Micro	osoft Windows Server	193.168.12.2
策略模板 任英			p-SVM-12	73	193.168.12.73	555	1	安全虚拟设备			193.168.12.2
计划任务	13	@ 1Cen	lerServer-1	270	193.168.12.70	0		虚频机	Micro	osoft Windows Server	193.168.12.2
次代定わ 役置	23	@ m-2	018-64		-	0		虚积机	-		193.168.12.2
	2	@ <u></u>	in7-32		-	0		虚积机	-		

图表 3-74

提示: 多个安全虚拟设备的授权计数之和不能超过授权证书许可的点数。

3.7 组件卸载

3.7.1 安全虚拟设备

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

□ 经结管理 ×)	B NAME	×	- @ ×
← → C Spups://19	3.168.12.8:294	s3/rvsmc/Bp/BpDetail?ep=423b6fdd=0a6f=c7fd=f4ed=f8e0f4becf73	\$ I
终端: Rising-SVM-12.			
 ○ 新成 ○ 新成 今 (新田白玉峰) ○ 承成 日志 七ろ 升ct 	τ. (ę	料理業務: #Rissg-GNA-1273 曲: 完全成策K 解題: 完全成策K 評題社: 1931661273 現日: 5557 動作業は: 未和 業業: 1.1.0 <u>空間分析</u> 単位:((2))	
	骤活状 态	чбыни: 193.168.1271 Год. Ейн≦ Фолон)
	- Seta	が現実現1:192108:12.222 重成につい 2 1个 身電:単位式名 ① 非式名	

图表 3-75

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

D 14488	× D Star B	× 🗖	- 0 ×
← → C Bb	HTS://193.168.12.8:2944	3/rvsac/Ep/EpDetail?ep=623b6fdd=0a6f=c7fd=f4ed=f8e0f4b	ec173 🕄 🗄
终端:Rising-	-SVM-12.73		
 ● 转端信息 ● 寄系 今:病面白名単 □ @ 末気 日志 任场 升道 	нада нада табба табба таб таб таб таб таб таб та	料紙名称: 約100-90%-1273	vm + RVS Test
	动 话的:出	vGhield: 193.168.12.71 代店: 水泥庙	#:5
	授职状态	所販業所: 19314412.222 主式CFU: 2 个 決選:寺 こだれ ○水 活れ	<u>信息 23</u> () 原始教派成功

图表 3-76

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

1 终端信息	×	_ @
93.168.12.8:294	3/rvsmc/Ep/EpDetail?ep=423b6fdd=0a6f=c7fd=f4ed=f8e0f4becf73	<u>ل</u>
ά th		9 Test
激活状容	v@Hald: 193168.1271 武士: 未敢者	激活
授权状态	所憲主戒: 193100/12222 宝萩のFPU: 2 个 余事: ○己既の ●未能化	截盘
	D thanks. D thanks. So that is a score of a scor	NBARA * NBARA * St. 168. 12. 0: 20445/rvsc/Rp/Rp/Detail/Rp/St.0421065640-0056-0726-264-64695404:2173 * 70 FRACES: Reside/State 1/200452173 R. 168. Reside/State 1/200452173 RES: Sc.dtBHK MEMORY Reside 1/200452174 RES: Sc.dtBHK MEMORY Reside 1/2014012222 RES/RES MEMORY Reside 1/2014012222 RES/RES

图表 3-77

提示:只能为开启状态的安全虚拟设备撤销授权。

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

	Sphere Client			
化件化)编辑化) 視目化)	清单 ② 系統管理 ④ 插件 ② 帮助 ③			
	8]清章 ▷ []] 主机构群集		·····································	
0 11				
· S wantoneannanu	WIN-LCHGBUHBVTO, 193.16	58.12.253 VMware vCenter Server, 5.0.0, 45	5964	
B 193.168.12.22	入门 前第中心 虚約総	主机《任务与事件》要指《权限》除制		
⊕ Info_Cenb ⊖ SiM ⊖ SiM	y 什么是主机和群集视题	图?	关闭选项卡	X
C) Imm C) SM E ⊕ Text Ø Where E ⊕ vSwidM C ⊕ Where	电理(1) ・ 客户机(2) ・ 快感(2) ・ 習 打开反制台(1)	集或资源地上运行的计算资源集构图可管理和组织计算资源的清	000	
ඩ Rising හි Wind හි Wind හි Wind	→ 締結役置(2) 対応の(2) 対応の(2)	_	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
CD WINZ CD WINZ CD WINZ	9 克隆(C) 模板(C) >	2	FARRENT	
C viva	Funlt Tolerance ()			
@ vCenter	虚拟机存储配置文件(8)			
() Wh2012 () Wh2012 () Wh7_12	添加积限(1) Cu1+f 警察(1) ,			
	报告性能(2)			
	重命名②		了解更多信息	
	在新窗口中打开(g) Ctrl+Alt+8 从演拳中移除(g)]] 了解更多有关清单视图的信息	
B###	从相差删除 (g)		名称、 贝谷	- ARM
				-

图表 3-78

安装与卸载



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

图表 3-79

3.7.2 其他组件

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





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。

马瑞星虚拟化系	统安全软件 □====================================	_02
墙里软件难扩铁	武區映	
瑞星软件维护	模式选项	
○添加/删	除())	
	根据您的需要,添加或删除产品的可选组件	
○修复(B)		
	为了修复产品,重新安装当前已安装的组件	
● 卸載 (U)		
	从电脑中卸载本产品	
	上一步 四 下一步 函 完成 四	取消(2)
		11

图表 3-81

第三步:确认卸载信息,点击【上一步】可进行修改,点击【下一步】继续。

🔜 瑞星虚拟化系统安全软件	>
安装信息 安装程序准备完成	20
请确认以下的信息是否正确。如果要修改信息,请单击 步"继续。	,"上一步"。单击"下一
当前信息:	
御戦的組代列機: 核心组件 管理中心 日志中心 重条肋作	<u>~</u>
I	r I
上一步 Q) 【下一步 Q】	完成② 取消②

图表 3-82



第四步:显示卸载进度信息。

马,瑞星度拟化系统 卸载过程中	安全软件	
	停止組件的应用程序 客户端日志代理组件 (&VSLOG)	
	上一步 (2) 下一步 (3) 完成 (2)	取消 ©

图表 3-83

第五步: 点击【完成】, 卸载结束。



图表 3-84

第四章 系统管理

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

4.1 管理中心

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





导航窗口:导航窗口包含树状结构的功能导航系统。

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

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

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

搜索:可以选择终端范围、设定组及其他搜索条件进行搜索。

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

瑞星虚拟化系统安全软件 | 51

2013/9/16 9:35:38



4.1.1 控制台

4.1.1.1 时间视图

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

fî	控制台	24小时视图 🔻		
终端范围:	所有终端	24小时视图 7天视图	RootGroup	

图表 4-2

4.1.1.2 Widget

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

V	警报状态	
V	警报历史记录	
V	我的账户状态	
V	染毒终端最新记录	
V	病毒趋势	
V	版本比例	
V	病毒最新记录	
V	授权情况	

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。

RACES NO	有线编 👻	RootGroup	7	6	推索

图表 4-4

4.1.2 警报

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

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

7987	101 85 FE 104	¥ Ro	störcup v	事件D:	RI第4 不規 ▼ 自 2013-06-01 下 03:00 ▼ 至 2013-06-01 下 00:00 ▼ 教育
3.10	949-02				
8	HA .	严重性	554K	事件の	用書
8	2013/8/1 21:59:45	日都市	vCentor	31401	由于有功的权不是。安全虚拟的2011年220的计事件包括因数
8	2013/9/1 17:59:27	⊖ ¥A	Win7_12.252(MC)	31000	繁重员adming152.158.11.53监罚头数。储良药10002
8	2013/0/1 17:37:52	⊖ ¥A	vCentor	31401	由于與功狀和不是。與全產的約.5%L_12.220的手帶於約.000於
8	2013/8/1 17:37:20	⊖ ØA	vCenter	31401	由于我的被你不是。我全意知识2012_22009并奉教校被回款
8	2013/9/1 17:20:17	⊖ ØA	vCenter	31401	由于我的抵抗不足。安全產與約5/14_12 230的杀秦族权被因除
Ð	2013/9/1 17:09:40	0 WA	vCenter	35421	由于我均质积不足。安全重复机5/14_12 2309并重度积减因积
8	2013/9/116:49:06	0.94	Ww7_12.252(MC)	39000	10里長40min,6,193,158,14,138至景兵舱,城県約10002
13	2013/0/112:00:00	Att N	S/M_12.233	6002	85M(系統升明時(1))(新生共務。編長将:(1)
13	2013/0/1 00:55 55	895	vCenter	31401	由于我的授权不足,安全编辑机论44_12.230的新潮损权被国际
8	2013/0/1 00:42:20	8.96	vCenter	31401	由于有均便很不是,安全虚拟现分和_12.23%的外事提供被国际
8	2013/8/1 00:48:48	0 W8	vCerNr	31401	由于有效供収不足,安全虚拟统9.44_12.230的分本提供被因款
8	2013/8/1 00:41.18	898	VCerNr	31401	由于有功则将不是,安全虚拟的7/4_122/01分离的时间的



勾选警报记录,点击 🔝 解除警报 ,可以删除该警报记录

	印度新闻				
2	时间 -	严重性	线锅	事件ID	内容
V	2013/8/15 17:54:21	□ 攀告	Win7_12.252(MC)	31000	管理员 admin 从193.168.18.115型录头数,描误码: 10001
	2013/8/14 17:54:28	□ 攀告	Win7_12.252(MC)	31000	管理员admin从193.168.14.26登录失败,锚误码:10002

图表 4-6



4.1.3 报告

报告分为【病毒疫情报告】和【系统状态报告】两类。

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



图表 4-7

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





图表 4-8

4.1.4 终端

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

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

楷	\$t:	® 23	¢ © IP A⊉	: 不限	v				6	指索
Ð	导入结谐(vCenter)	© 5624	▶ ₀ ,移动到	x 不職	1 4	A、开始杀毒 🕵 停止杀毒 🖪	教权分配			
	名称		IP	虚拟主机 安全虚拟设备	2.2	操作系统	ESXI	重本	授权占用	状态
Ð	₿ 193.168.12.221		-	虚拟机	R	VMware ESXi 5.0.0 build-4	-	-	-	-
800	And the second secon			物理机				*****		***



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。

www.es78 • NBRD: NA •							a - 18	sean
新聞· ● 210:0 P 典型· 738	*						1	投た
SYTEMPCented	✿ 2,8740	0, пыка	R. 61268	医 服用分配				
1 2/8 A	P	9403	22	静压系统	E\$30	(数)	教权占用	就靠
B 193 168 12 221	-	0	虚拟主机	Villware ES9 5/0.0 build-469512	-	-	-	-
B 20100617-1753	193.168.18.153	8801	them.	-	-	1.0.0.7	-	œu.
D 2206-1245	-	0	dim.	-	193.168.12.221	-	-	胞液
B PRCTest	193.168.18.77	8868	REEN		-	1.0.0.1	-	胞线
D 514 12.230 (5141)	193.168.12.230	5557	安全虚拟机	其他 2.6 a Linux (64 位)	193.158.12.221	1.1.8	2	₫Ø.
B Test env 12.21 (test-env-f)	193, 168, 12, 21	0	dirin.	其他2.6xLinux(64位)	193.168.12.221	-	-	胞液
් <i>ම හාස</i> ා	-	0	discon.	-	193.158.12.221	-	-	胞状
B UppaterCenter, 12.24 (VIII)DOUG-81139520.	193.158.12.24	29010	datas.	Morosoft Mindows Server 2008 R2 (64 (2)	193.158.12.221	1.0.0.5	-	GUE.
	193.168.12.116	0	den	Microsoft Mindows Server 2008 R2 (54 (2)	193.164.12.221	-	-	胞液
D D STIRIGHARASSE	-	0	diren.		193.158.12.221	-	-	胞线
B 10420003084 12.16 (ROSING-3CE10213)	193.158.12.15	8510	diren.	Microsoft Mindows Server 2003 (54 位)	193.158.12.221	01.00.00.01	-	15 15
B 1002000000 12.20	193, 168, 12, 20	29010	anten.	Microsoft Windows Server 2003 (32 位)	193.168.12.221	1.0.0.0	-	and a
		具 20 表记录 111	4±-3	1 下一八) 4次世示 100 - 糸				

图表 4-10

系统管理

4.1.4.1 组

导航窗口显示的终端组分为三类,包括 vCenter 导入组 2, 自定义组 3, 剩余组 3 。其中:

4.1.4.1.1 vCenter 导入组

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



图表 4-11

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

组信息

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

56 | 瑞星虚拟化系统安全软件

2013/9/16 9:35:39

基本信息			
	组名称:	vCenter(193.168.12.116:443)	
	层级:	RootGroup + vCenter(193.168.12.116:443)	
	组类型:	vCenter管理中心	
vCenter & vShiel	d		
	vCenter地址:	https:// 193.168.12.253 : 443 /sdk	
	用户名:	administrator	
	密码:		
	vShield抱止:	https:// 193.168.12.254 : 443 /api	
	用户名:	admin	
	密码:		保存

图表 4-12

警报

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

【杀毒】显示组相关扫描、文件监控和隔离区策略信息。

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

479.4**				
扫册	文件监控	隔离区		
隔离区设置				
隔离区空间不	足时: ④ 空间自动	が 個长 ◎ 礼	换最老的文件	
Phil	<u> </u>	мв		
	隔离区设置隔离区空间不隔	隔离区设置 隔离区空间不足时: @ 空间自动 隔离区大小: 500	隔离区设置 隔离区空间不足时: ● 空间自动增长 ● 普 隔离区大小: 500 MB	隔离区设置 隔离区空间不足时: ③ 空间自动增长 ◎ 普換最老的文件 隔离区大小: 500 MB

图表 4-13

查杀日志

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

隔离区

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

瑞星虚拟化系统安全软件 | 57

2013/9/16 9:35:40

系统管理

日志

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

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

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

4.1.4.1.2 自定义组

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



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 (2) 删除 进行终端的移动和删除操作,点击 合 立即升级进行终端组件的升级。

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

4.1.4.1.3 剩余组

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

4.1.4.2 虚拟主机

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

终端信息

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

基本信息					
	终端名称:	193.168.12.221	1		
	类型:	虚拟主机			
	所属组:	RootGroup + V	Center(193.168.12.116:4	443) ► Data ► host	
	IP地址:	未知			
	;;;口:	0			
	操作系统:	VMware ESXi 5	.0.0 build-469512		
	版本:	未知	立即升级		
	备注:]	保存

图表 4-15

警报

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

日志

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

任务

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

4.1.4.3 安全虚拟设备

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

终端信息

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

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

甘大伴用							
至中區思							
L	终端名称:	Rising-SVM	-12.73				
在线	类型:	安全虚拟设计	ł				
	所属组:	RootGroup	▶ vCenter	(193.168.12.70	443) + Datace	enter + vm +	RVS Test
	IP地址:	193.168.12	.73				
	编口:	5557					
	操作系统:	未知					
	厳本:	1.1.8		立即升级			
	备注:						保存
激活状态							
	vShield :	193.168.12	.71				
	状态:	己邀活					撒纳激活
授权状态							
	所属主机:	193,168,12	222				
	##CPU:	21					
	200000	* . *	0 + 19 In				
	余毒:	98 日投权 19	◎未預収				ARCE

图表 4-16

警报

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

病毒白名单

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

全部清空 ,	删除全部病毒记录。
--------	-----------

		全部3
病毒名	病毒ID	擾作
ojan.PrettyPark	1073748535	1919
rojan.BO	1073753547	粉除
rojan.Win32.Generic.522BCA30	1378601520	静脉

图表 4-17

日志

【日志】显示安全虚拟设备相关日志记录,具体操作方法请参考本文档章节

4.1.6.1 日志。

任务

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

升级

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

🔲 继承组	策略						
	升级	日志					
目定時	讨设置						
V	启动定时升级	3					
	☑ 周日	☑ 周—	☑ 周二	☑ 周三	☑ 周四	☑ 周五	☑ 周六
	开始时间:	12:00 🔻					
■ 升紙	3方式设置						
■ 网络	¥连接设置						
			8	表 4-18	3		

4.1.4.4 虚拟机

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

终端信息

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

各语思					
	终端名称:	WinXP_12.15			
在线	类型:	虚拟机			
	所属组:	RootGroup + vCenter(193.168.12.116:443) + Data + vm			
	IP地址:	193.168.12.15			
	端 口 :	29010			
	操作系统:	Microsoft Wind	ows XP Professional (32 位)		
	版本:	1.0.0.8	立即升级		
	备注:	RISING-D81CI	E95A		保存

图表 4-19

系统管理

警报

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

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

日志

任务

升级

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

4.1.4.5 物理机

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

4.1.5 杀毒

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

4.1.5.1 杀毒策略

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

4.1.5.2 查杀日志

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

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

62 | 瑞星虚拟化系统安全软件

2013/9/16 9:35:40

处理结果

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

【清除失败】因各种可能的原因而无法清除病毒。

【删除成功】已删除受病毒感染的文件。

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

【查杀失败】因各种原因可能导致查杀失败。

【已忽略】未采取任何处理措施,但记录了对病毒的检测。

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

1 10 10 10 10 10 10 10 10 10 10 10 10 10	在杀日志					
终端范围: 所有约:	K v	RootGroup	* 病毒共型: 不詳	▼ 处理結果:	不課・	NE
病毒名称:		发现时间: 不须 * 白	2013-08-18 🖬 00:00 🔻	· 至 2013-08-18 [00.00 -	
重利利用	9EW	P	病毒名	京専会型	染毒文件	处理结果
2013/8/11 18:57:42	Win7x86_12.17	193.168.12.17	Weather.A	能分量	C:Users\Administrator/Desk	重杀失败
2013/0/11 10:50:59	Win7x86_12.17	193.168.12.17	Melissa.0	総杂型	C:Users\AdministratorDesk	重杀失数
2013/8/12 18:59:16	Win7x06_12.17	193.168.12.17	Melissa.0	超杂型	C:Users\Administrator/Desk	童杀失歌
2013/8/12 18:59:16	Win7x86_12.17	193.168.12.17	Melissa.B	総合型	C:Users\Administrator/Desk	室杀失歌
2013/8/12 18:57:09	Win7x86_12.17	193.168.12.17	Wazzu AB	然유럽	C:Users\Administrator/Desk	室半共敗
2013/8/12 18:59:16	Win7x86_12.17	193.168.12.17	Melissa.B	読み型	C:Users\AdministratoriDesk	童米失敗
2013/8/11 18:58:59	Win7x86_12.17	193.168.12.17	Melissa.B	然杂型	C:Users\Administrator/Desk	童杀失敗
2013/8/12 18:57:09	B Win7x86_12.17	193.168.12.17	Melissa.B	總杂型	C:Users\Administrator/Desk	童杀失败
2013/8/12 18:59:17	B Win7x86_12.17	193.168.12.17	Melissa.B	成杂型	C:Users\AdministratoriDesk	童杀失敗
2013/8/12 18:57:09	@ Win7x06_12.17	193.168.12.17	Melissa.0	15.00 B	C:Users'Administrator/Desk	童杀头歌
2013/0/12 10:59:17	@ Win7x06_12.17	193.168.12.17	Melissa.0	1592	C:Users\Administrator/Desk	童杀头歌
2013/8/11 18:57:43	Win7x96_12.17	193.168.12.17	Wazzu.AB	總杂盟	C:Users\Administrator/Desk	室杀失敏
2013/8/12 18:57:10	Win7x86_12.17	193.168.12.17	Melissa.B	整杂型	C:Users\Administrator/Desk	室半共歌
2013/8/12 18:59:17	B Win7x86_12.17	193.168.12.17	Melissa.B	感染型	C:Users\Administrator/Desk	皇半失敗
2013/8/11 18:57:43	@ Win7x86_12.17	193.168.12.17	Wazzu.AB	國유럽	C:Users\Administrator/Desk	童长失敗
2013/8/11 18:58:59	B Win7x86_12.17	193.168.12.17	Melissa.B	總杂型	C:Users\Administrator/Desk	重杀失败
2013/8/12 18:58:04	Win7x86_12.17	193.168.12.17	Wazzu AB	然 杂型	C:Users\Administrator/Desk	重杀头教

图表 4-20

4.1.5.3 隔离区

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

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

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

瑞星虚拟化系统安全软件 | 63

2013/9/16 9:35:40

	病毒隔离	×					
150	CODE: MANA	▼ RootGroup	×	病毒名称:		病毒突型: 不限 マ	216
MA	財通: 不限 マ 日	2013-08-18 🔳 00:00	₩ 至 2013-08-18 ■	00.00 *			
-	的意味是这件						
	网络时间	- 10 8	IP	梁蜀文件	大小	A#6	病毒类型
	2013/8/18 02:36:05	B WinXP-SP3-32_liud	193.168.12.231	c\documents and settings	176.5K	Win32.FunLove	未知
8	2013/8/18 02:35:05	WinXP-SP3-32_liud	193.168.12.231	c\documents and settings	57.2K	Win32.HPS	未知
1	2013/8/18 02:36:05	WinXP-SP3-32_Bud	193.158.12.231	c\documents and settings	176K	Win32.FunLove	未知
8	2013/8/18 02:36:03	B WinXP-SP3-32_Bud	193.158.12.231	c'documents and settings	57.5K	Win32.HPS	未知
8	2013/8/18 02:33:21	B WIN/P-SP3-32_Bud	193.168.12.231	c'ittpe_funiove.exe	176K	Win32.FunLove	未知
8	2013/0/10 02:33:21	B WinXP-SP3-32_Bud	193.168.12.231	c'ittpe_hps.exe	57.2K	Win32.HPS	未知
	2013/8/18 02:33:18	B WINXP-SP3-32_Bud	193.168.12.231	c:mpehfs.exe	57.5K	Win32.HPS	未知
в	2013/8/18 02:33:17	B WINXP-SP3-32_Bud	193.168.12.231	c'illipefun.exe	176.5K	Win32.FunLove	未知
8	2013/8/16 21:21:48	WinXP-SP3-32_liud	193.168.12.231	c\documents and settings	114K	Trojan.BO	木马
	2013/8/16 21:21:48	B WinXP-SP3-32_Bud	193.168.12.231	c\documents and settings	35.8K	Trojan.PrettyPark	木马
8	2013/8/16 21:21:47	WinXP-SP3-32_Bud	193.168.12.231	c\documents and settings	203.7K	Trojan.Win32.Generic.522BCA30	木马
8	2013/8/16 20:59:40	B WinXP-SP3-32_Bud	193.158.12.231	c'documents and settings	203.7K	Trojan Win32 Generic 522BCA30	木马
8	2013/8/16 20:59:30	B WIN/P-SP3-32_Bud	193.168.12.231	c'idocuments and settings	114K	Trojan.BO	木马
	2013/8/16 20:59:30	B WWWP-SP3-32_Rud	193.168.12.231	c\documents and settings	35.8K	Trojan.PrettyPark	木马
	2013/8/16 20:59:20	B WinXP-SP3-32_Rud	193.168.12.231	c\documents and settings	35.8K	Trojan.PrettyPark	木马
8	2013/8/16 20:59:20	B WAXP-SP3-32_Rud	193.168.12.231	c\documents and settings	35.8K	Trojan.PrettyPark	木马

图表 4-21

勾选隔离区文件信息,点击 冊 恢复隔离文件,可以将隔离文件恢复到终端上。

4.1.6 系统

4.1.6.1 日志

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

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

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

E	∛ 8±				
19K	1999: 所有终端	٣	RootGroup	严重性: 全部	× \$80:
时间	· 不親 * 日 2013-0	0-10 🔳	00:00 * 至 2013-08-18 至 00:0	0 ¥	
	16月 - *	严重性	NGR .	事件ID	内容
8	2013/8/19 04:13:33	48	Win2008_12.23(UC)	41013	升级到10.0.12版本失败。原因: 總件攝送文件加數失敗
8	2013/8/18 19:15:47	住息	Win7_12.252(MC)	21307	管理员adminizicimpents.exe等1个文件创建了隔离区恢复任务
8	2013/8/18 16:44.01	48	Win7_12.252(MC)	21004	管理员admin经改了个人信息
8	2013/8/18 16:35:14	118	Win7_12.252(MC)	21000	管理员admin从193.163.11.73至录成功
8	2013/8/18 12:00:05	a e	WinXP-SP3-32_liud	41001	升级到1.0.0.12数本失敗・原因: 高戶端已经是最新版本
8	2013/8/18 09:31:10	住息	UpdateCenter_12.24	41012	升级到1.0.0.12版本失敗・原因: 用户取消升级
8	2013/8/18 09:31:07	48	Win7_12.252(MC)	41013	升级到1.0.0.12版本决股・原因: 総件価述文件加数失敗
8	2013/8/18 04:14:15	48	Win2008_12.23(UC)	41013	升级到1.0.0.12版本失敗・原因: 細井描述文件加数失敗
8	2013/8/18 02:41:48	48	Win7_12.252(MC)	21305	管理员admin时WinXP-SP3-32_liud等1个目标创建了病毒重杀(ODS)任务
8	2013/8/18 02:41:27	118	Win7_12.252(MC)	21205	管理员admin设置了终端WinXP-SP3-32_liuz的杀毒策略
8	2013/8/18 02:41:27	住息	Win7_12.252(MC)	21207	管理员admin设置了终端WinXP-SP3-32_liuz的强度区策略
8	2013/8/18 02:37:30	住息	Win7_12.2523MC)	21205	管理员admin设置了终端WinXP-\$P3-32_luc的杀毒猪略
8	2013/8/18 02:37:29	住息	Win7_12.252(MC)	21207	管理员admin设置了终端WinXP-SP3-32_luc的预期区策略
8	2013/8/18 02:35:45	住民	Win7_12.252(MC)	21205	管理员admin设置了终端WinXP-SP3-32_liuz的杀毒策略
8	2013/8/18 02:35:45	48	Win7_12.252(MC)	21207	管理员admin设置了终端WinXP-SP3-32_Iuc的装置区策略
8	2013/8/18 02:33:00	48	Win7_12.252(MC)	21305	管理员admin對WinXP-SP3-32_liud等1个目标创建了病毒查杀(ODS)任务
8	2013/8/18 02:24:48	118	Win7_12.252(MC)	21305	管理员admin对WinXP-SP3-32_liud等1个目标创建了病毒查杀(ODS)任务

图表 4-22

4.1.6.2 用户

用户是指管理中心帐户持有者。

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

2						
0 812	O 103 b 1	透金码				
	用户名	£	角色名称	上次臺景时间	上次醫業IP	状态
	admin	System Admin	Administrators	2013/8/18 19:47:42	193.168.11.73	启明
8	audit	审计管理员。测试用	Administrators	2013/8/16 23:39:40	193.158.14.8	启用

图表 4-23

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

新増					23
用户名:					
密码:					
确认密码:					
备注:					
语言:	简体中文	-			
角色:	Administrators	•			
状态:	◉启用	◎禁用			
				确定	取消

图表 4-24

提示:角色信息请参考本文档章节 4.1.6.3 角色。

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

系统管理

提示: admin 帐户无法删除

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

4.1.6.3 角色

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

角色窗口显示所有角色,角色信息包括角色名和用户数。

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



图表 4-25

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

新增					:
角色名:					
权限谈定:	系统设置:	◎无权限	◎只读	◎读写	
	用户:	④无权限	◎只读	◎读写	
	终端:	④无权限	◎只读	◎读写	
	报告:	④无权限	◎只读	◎读写	
	系统日志:	●无权限	◎只读	◎读写	
	警报:	④无权限	◎只读	◎读写	
	授权:	◎无权限	◎只读	◎读写	
	策略:	④无权限	◎只读	◎读写	
	任务:	④无权限	◎只读	◎读写	
	病毒日志:	④无权限	◎只读	◎读写	
					確定 取消

图表 4-26
勾选角色信息,点击工具栏中的 区 删除 ,可以进行角色的删除操作。

提示:系统管理员角色无法删除。

4.1.6.4 策略模板

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

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

策略模板信息支持条件搜索,可选条件为产品。

4品: 不課		*				
) SERVICE	S 90000	O BUSKE				
	解職名称		产品	分类	已分散地	已分配時間
123		杀毒		杀毒菌的	0	0
toball		杀毒		杀毒菌酸	0	0
MEL		终端代理		代理解解	0	0

图表 4-27

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

分配模板			23
分配到组	分配到终端		
日 日 日 日 日 日 日 日 日 日 日 日 日 日	93.168.12.116:443) t new-folder 己发现虚拟机	RootGroup	
			确定取消

图表 4-28

系统管理

点击工具栏中的 ③ 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。

策略名称:			已分配例:	
第四典型: 永寧		-		
内容				
お摘 文件	當控			
n setta				
the state of the second s				
E 启动定时扫描				
■ Astrice##3編 図 用日 図 用	- 12 AL		1 👿 周五 👿 周六	
 島地営村3届 図 用日 図 用日 図 用日 12:00 	- 図月二 -	🛛 R.E 🛛 R.	9 國 與五 國 與六	
总达会时打3篇 区 用日 区 用 开始时间: 1200	- 18 A-	12 RE 12 R	1 図 月五 図 用六	
 E 自动向时扫描 区 用日 区 用 开始时间: 1200 日 建筑 G 扫描完型设置 	- V A-	80 R.I. 18 R	1 図 用五 図 用六	

图表 4-29

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

4.1.6.4.1 扫描策略

定时扫描

配置定时扫描的启用状态和开始时间。

目 定时扫描 ······						
🔲 启动定时扫	描					
☑ 周日	🛛 周—	☑ 周二	☑ 周三	☑ 周四	🗹 周五	🔽 周六
开始时间:	12:00 🔻					

图表 4-30

病毒处理选项

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

68 | 瑞星虚拟化系统安全软件

2013/9/16 9:35:41

Ξ	选项			
	发现病毒时处理方式: 🔘 清除	◎ 删除	◎ 忽略	
	查杀文件不大于MB			
	查杀文件层数不大于层			
	■ 开启智能提速			

图表 4-31

扫描类型设置

配置安全级别,定义扫描文件类型和病毒类型。

安全级别: ● 本 ● 本 ● 自定义 文井夫型 ● 御道文件 ● 御道文件 ● 御道文件 日本市文中 ● DOS司以行文件 ● Minoreally行文件 山山山司以行文件 ● 宏文件 未永成文件 ● 御道文件 ● 香道文件 未永成文件 ● 御道文件 ● 香道文件 未永御本文件 ● 御道文件 ● 香道文件 ● 新道文件
文件类型 節範文件 節範文件 節範文件 節新文件 百元或文件 DOS司队行文件 DOS司队行文件 Winforwa司队行文件 山山の司执行文件 意文件 未未成文件 朝本文件 蓄蓋文件 未未成以件 朝本文件 普通文件 未未成以件 ● 範疇区次件 ● ●
丘疝文件 創稿文件 創件文件 希売文件 DOSQN(打欠件 windowsQN(打欠件) UnunQht文件 素文件 未成文件 製本文件 書畫文件 未加厚本文件 自病正文件 書書文件 年加厚本文件
副和交文件 DOS词从行文件 Windows词从行文件 Unuxi司执行文件 意文件 景本级文件 脚本文件 普查文件 景本级学文件 自新正文件 普查文件 景本城学文件
Unuraphyf文件 宏文件 未秋度文件 脚本文件 番茄文件 未知即本文件 自新正文件 番茄文件 未知即本文件
□ ψ本文件 番茄文件 未知與本文件 □ 前庭文件 □ 前庭文件
一 会事并刑
L Maxe
未知DOS病毒 未知Windows病毒
□ 未知引导型病毒 □ 未知木马

图表 4-32

自定义查杀目标

配置扫描的文件扩展名和目录。







自定义排除查杀目标 配置排除扫描的文件扩展名、目录和全路径。

自定义排除查杀目标	
扩展名:	提示:
	文件扩展名:
	XYZ 示例: doc, 如包含多个扩展名, 以回车隔开
	目录:
日录.	XYZ 示例: C:IProgram Files,如包含多个目录,以回车隔开
日本:	包含通配符(*)目录:
	*** 示例: C:\Program Files**
	文件全路径:
	XYZ 示例: C:Program Files/test.bt
文件全路径:	注释:
	XYZ#注释示例: doc#揭除.doc文件



4.1.6.4.2 文件监控策略

文件监控选项

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

☑ 开启监控	
■ 选项	
发现病毒时处理方式: 🔘 清除 🛛 🔍 删除	◎ 忽略
查杀文件不大于MB	
查杀文件层数不大于	
■ 开启智能提速	

图表 4-35

扫描类型设置

自定义查杀目标

自定义排除查杀目标

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

70 | 瑞星虚拟化系统安全软件

2013/9/16 9:35:42

4.1.6.4.3 升级策略

定时设置

配置定时升级的启用状态和开始时间。

目 定时设置						
🔲 启动定时升	级					
☑ 周日	☑ 周—	☑ 周二	☑ 周三	☑ 周四	🗹 周五	🗵 周六
开始时间:	12:00 💌					

图表 4-36

升级方式设置

配置升级源地址。

- scottige 1.0	0 18AE/18X19C	
服务器地址:		
端口:		

提示: (服务器地址为IP地址或主机名或域名)



网络连接设置

配置网络连接方式。

◉ 直接连接	◎ 代理连接		
服务器地址:		٦	
端口:			
🗹 身份验证			
用户名:			
密码:			

提示: (服务器地址为IP地址或主机名或域名)

图表 4-38



4.1	.6.4.4	日志策略
-T.1	.0	

日志中心

配置日志中心地址。

服务器地址:			
3端口:			

图表 4-39

4.1.6.5 任务

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

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

任务 任务					
线端范围: 所有终端	▼ RootGroup	▼ 任务类型: 不限	*		82
创建时间: 不訊 🔻 🔒	2013-08-18 🔳 00:00 💌 🕱 2	013-08-18 🔳 00:00 👻			
Ektestill	▼ 类型	的服人	状态	进度	详任
2013/8/18 21:17:57	病毒壹杀(ODS)	admin	完成		室垂
2013/8/18 21:15:56	病毒 宣杀(ODS)	admin	完成		童戲
2013/8/18 19:15:47	隔离区恢复 谨慎	admin	完成		室板
2013/8/18 09:31:04	升级中心两步	admin	执行中		亚航
2013/8/18 02:41:48	病毒查杀(ODS)	admin	完成		東南
2013/8/18 02:33:00	病毒宣杀(0DS)	ədmin	完成		聖戲
2013/8/18 02:24:48	病毒查杀(ODS)	admin	完成		東 戴
2013/8/18 02:22:52	病毒壹杀(ODS)	admin	完成		室敷
2013/8/18 01:40:15	病毒查杀(ODS)	admin	完成		重新
2013/8/18 01:20:25	病毒查杀(ODS)	admin	完成		東直
2013/8/18 01:18:41	病毒宣杀(0DS)	admin	完成		聖藝
2013/8/18 01:17:16	病毒查 杀(ODS)	admin	完成		亚兹
2013/8/18 01:13:57	病毒查杀(ODS)	admin	完成	-	聖戲

图表 4-40



点击任务事件详情查看链接,显示任务完整信息。

任务详情					
常规					
任务类型:	病毒查杀(ODS)				
创建人:	admin				
创建时间:	2013/8/18 21:17:57		完成(100%)		#28#(0%)
完成度:	等待:0				执行中(0%)
	执行中:0				等待(0%) 失败(0%)
	完成: 1(1成功/0失则	2)			
	超时:0				
\$	冬湖 🔺	IP	状态	完成时间	错误码
WinXP-SP3-32	2_liuzi	193.168.12.231	完成	2013/8/18 21:18:44	0

图表 4-41

4.1.6.6 计划任务

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

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

0	和建计划任务 🐻 启用	10 M.F	O BER			
	名称		発想	创建人	时间计划	8K3
3	shengillongbu	Ħ	股中心開步	admin	周-/二/三/12:00	自
5	5555555	Ħ	股中心两步	admin	周日/-/二/三/四/五/六/09:31	白明
3	每天中午空时升级	纲	a升级	admin	周-/二/三/四/五/12:00	\$1.0

图表 4-42

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

点击工具栏中的 ① 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。

系统管理

双 符名称:			时间计划:	CRO CR- CR	- 88- 888 885 8	周六
2:	终端升级	¥		12.00 -		
行目标						
196218:	記念法		模定终端:			
803	RostGroup			名称	* 1P	
	- Center 193 168 12 1163	(443)	E 16	193.168.12.221	-	
E	B host	vCenter(193.168.12.116:443)	8	20100817-1753	193.168.18.153	
	回避 new-folder 回避 已知我會採税		E 🕹	DSVA-12.46	-	
				PMC Test	193.168.18.77	
	■ 服务器		0.00			
	■ 服务器		E @	Rising-SVM	-	

图表 4-43

4.1.6.7 授权证书

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

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

授权证书				
3 导入授权				
产品	授权许可号	有效日期	授权点数	状态

图表 4-44

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

4.1.6.8 设置

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

💭 系统设置					
默认升级中心					
升级中心列表:	193.166.12.23:29088				
	第5番: 3歳日: 22008 0 月前				
日志中心					
日志中心列表:	☐ 193.168.12.252.1203				
	施行器: 30085 〇 圳加				
放掘青理					
自动囊除早于以下时间的病毒宣杀日志:	60天 ×				
自动请除早于以下时间的病毒隔离日志:	90天 👻				
自动直接早于以下时间的系统事件日志:	30天 *				
自动调除早于以下时间的任务:	15天 👻				

图表 4-45

4.2 安全虚拟设备

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

🔁 193. I	68.20.2	0上的1	lising	SV			_ 🗆 ×
文件(2)	視田の	虚拟机	D				
		10 8	1 64	MR	0	Ho .	
		0	in Dali	610 eC	~	N/	
	r						
		_	_	_	_		
						Rising Virtual Security	
		_	_		_		
					L	og inName:	
					p.	assuord :	



4.2.1 系统信息

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



图表 4-47

系统管理

4.2.2 配置管理网络

选中【Network】页签,显示【Network Interface】管理安全虚拟设备网络地址。 安全虚拟设备缺省使用本地 DHCP 服务器分配的 IP 地址。如果没有 DHCP 服务器,回车后手动输入 IP 地址信息。

193. 168. 20.	20上的 Rising-SVI	_10
文件(2) 視園(的電影和の	
00 🛛		
	Rising Virtual Security Setting Utility	
	System Network User Advanced Logout	
	· · · · · · · · · · · · · · · · · · ·	
	Network Interface	
	IP address : 193.168.28.225	
	г Network ipv4 Setting : 193.168.28.2	
	: 4.4.4.4	
	IP address :	
	Netwask : Default Gateway:	
	Primary DNS :	
	Secondary DNS :	
	Enter Enter Command Op/Down Select (tem Alt+F2/Alt+F1 Terminal in/out Esc Exit Left/Right Select Menu Ctrl+Q Logout	

图表 4-48

4.2.3 配置密码

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

्री 193, 168	3.20.20	上的 Riv	ing-SV							-0
文件(2) 社	188 C)	虚拟机业								
. 00		00	(h 1	88	۵ 🖗					
	5	Sustem	,	R	ising Vir	tual Secur	ity Set	ting Utility		
		,								
	2	Set Use	r Pas:	sword		_	this	will change	the password	
			A		II. alberra	0-1		014 . 50 (014 .)	Terrature 1	1
	Ent	Ex	it Co	DMMand	Left/Ri	ght Selec	t Menu	Ctrl+Q	Logout	In/out

图表 4-49

4.2.4 重启系统

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

Syst	ем Netwo	Rising Virtual rk User	l Securi Adv	ty Set anced	ting Utility Logout		
Rebo	с Off ot System			tttt Hach	Harning!!! ine will ромет	off	
Enter Esc	Enter Comman Exit	d Up/Down Left/Right	Select Select	Item Menu	Alt+F2/Alt+F1 Ctrl+Q	Terminal Logout	in∕out

图表 4-50

4.2.5 退出系统

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

Syst	ем	Ri Network	sing Virtual User	Securi: Adv	ty Set anced	ting	Utility Logout		
Jser	Logou	2			1111 sett	Warni ing ы	ng†††		
Enter	Enter	Соммала	Up/Down Left/Right	Select	Item Menu	Alt+ Ctrl	F2/Alt+F1 +0	Terminal Logout	in/out

图表 4-51

4.3 管理工具

4.3.1 远程安装工具

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

是客户端远程安装工具	×
注意:从左拦中选择需要运程交换的计算机 在中,你可以直接在编辑组中输入式计算 「 ¹⁹ 合资源 日 -	添加到右栏,如果你要安装的计算机块有出现在左 名或III,然后点击"添加"。
朝 第2 第2 第2 第2 第2 第2 第2 第2 第2 第2 第2 第2 第2	系 □ ・ 副計
<▶ 计算机名或IP: 	

图表 4-52

4.3.2 **域脚本安装工具**

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



图表 4-53

4.3.3 **隔离区管理工具**

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

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

操作 选择 查者 工具 帮助 田原 语空 朝新 设置空间 アクた 原始なが、 「原始なが」 「原始なが」	
田院 清空 期新 设置空间 7.26 1 <td< th=""><th></th></td<>	
夕砂 原設公 原室时间 库主名称 十人	
1/2 1/2 1/2 1/2 1/2 1/2 1/2 1/2 1/2 1/2	

图表 4-54

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

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

【查看】 执行查看,包括刷新列表、查看病毒资料和列项目。

【工具】 执行设置,包括设置隔离区空间、设置隔离区目录和设置硬盘保留 空间。

福度区剩余大小	硬盘剩余空间		
500.00 MB	隔离区大小	500	MB
高离区突然间已满时	硬盘剩余空间	479	MB
C 空间自动增长	硬盘保留空间	1000	MB
● 替换最老的文件	总计	1979	MB
设置隔离区目录			
C:\RV5BIN		浏	览
	确定	取消应	用

图表 4-55

杀毒

第五章 杀毒

5.1 手动查杀

操作步骤

- 启动并登录瑞星虚拟化系统安全软件管理中心控制台;
- 点击左侧导航窗口中的【终端】,显示所有被管理的终端;
- 勾选需要查杀的虚拟机终端,点击工具栏 Q 开始杀毒;
- 查杀过程中,可以随时点击工具栏 🕢 停止杀毒,终止查杀病毒;
- 当查杀病毒时, 点击【查杀日志】, 实时查看查杀记录;

● 查杀结束后,全部查杀日志将自动保存,可以通过在查杀日志窗口中设定不同的搜索条件来查询特定的信息。

查杀策略设置请参考本文档章节 4.1.6.4.1 扫描策略。

5.2 文件监控

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

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

监控策略设置请参考本文档章节 4.1.6.4.2 文件监控策略。

附录一 北京瑞星信息技术有限公司简介

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

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

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

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

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

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

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

瑞星虚拟化系统安全软件 | 81

2013/9/16 9:35:43

附录

附录二 瑞星信息安全资讯网

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

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

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

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