瑞星虚拟化软件 FOR VMware 常见问题

Q&A

北京瑞星信息技术股份有限公司

2015 年 12 月 3 日

目录

一、 产品构成基础问题

1. 虚拟化产品包装中由那些文件组成？

- 快速使用指南
- 客户服务指南
- 注册扩容指南
- 安装光盘和资料盘

产品序列号在安装光盘上，在后续的瑞星虚拟化管理控制台还需要产品授权文件，请参考【注册扩容指南】在瑞星官网注册，并下载授权文件，否则无法正常使用。

2. 如果发现安装光盘无法正常读取了，该如何安装产品？

在将产品序列号在官网注册完成后，会获得对应该注册产品的唯一【服务号】，请使用该【服务号】登录瑞星虚拟化产品自助平台，下载安装文件即可。

3. 为什么虚拟化产品的扩容号比基本包序列号少一组？

产品授权体系设计如此，并不是扩容号有问题。基本包号由 5*5 组，25 位序列号构成，扩容包由 4*4 组，16 位序列号构成。

4. 虚拟化产品扩容后，是否还需要重新导入授权文件？

当获取到扩容号后，必须要在瑞星官网的瑞星虚拟化自助平台上使用原产品的【服务号】登录扩容，具体操作请参照【注册扩容指南】。扩容注册完成后，必须重新下载扩容后的网站授权文件，并导入到瑞星虚拟化控制台（PMC）中，才可正常使用扩容后的产品。

二、 瑞星虚拟化软件 VM 产品常见问题

1. 文档内名词解释

【PMC】=瑞星虚拟化 WEB 管理控制台

【SVM】=瑞星虚拟化安全虚拟设备（OVA 模板虚拟机形态）

【GVM】=虚拟机

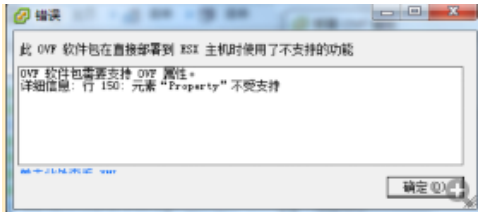
【ESXI】=可简单理解为 VMware 物理主机

【VMware vshiled manger】=专为 VMware vCenter Server 集成而构建的安全虚拟设备套件

【vshiled Endpoint】=用于保护物理基础架构的管理界面还可以用来管理虚拟化环境的防病毒和防恶意软件策略插件。（依赖于 VMware vshiled manger）

【VMware DRS】=为虚拟机提供动态平衡和资源分配。

2. 导入 SVM OVA 文件报错，如何处理？



需要使用 vSphere Client 链接 vCenter Server 进行部署，不要使用 vSphere Client 直接链接 ESXi 进行部署。

3. 打开 vshiled manger 时报错，如何解决？

此问题请在 vcenter 导入 vshiled manger 后耐心等待，如果一直无法打开页面，请尝试导入部署 vshiled manger，如果依旧无法解决，请联系 vmware 厂商人员处理。

4. vshiled manger 部署 endpoint 非常缓慢？

该问题瑞星方面无法解决，是由于 VMware 可能这方面体验做的不太友好引起，endpoint 在安装过程中确实会非常慢，这个只能等待 VMware 进行优化。但有几个建议提供给大家：

- 尽量使用 google chrome 或火狐浏览器登录 vshiled manger 安装 endpoint 组件，成功率会相比 IE 高出很多。
- 当点击安装后切勿刷新浏览器页面，耐心等待即可。
- 务必保证 vshiled manger 与 vCenter 之间的网络通信。

5. 瑞星虚拟化 VM 产品所需端口（默认端口）

- 管理：29443
- 通信：29121
- 其他：29080

升级中心

- 通信：29088

日志中心

- 通信：29086

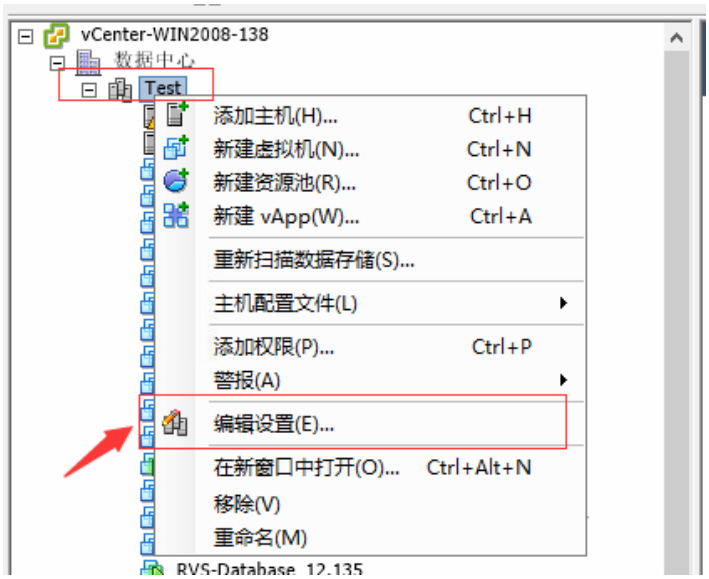
MySQL 数据库

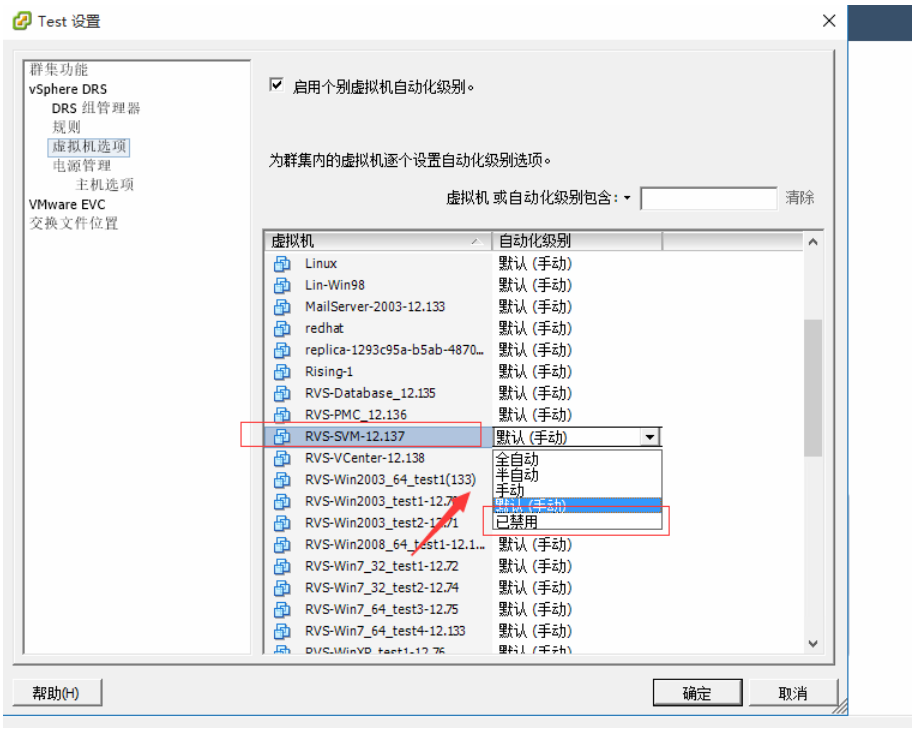
- 通信：3306

6. SVM 在使用中经常出现在虚拟机中漂移的问题？

往往部署了 VMware 的用户环境，都会开启 DRS 功能以保证服务器高可用，故导致在群集中的一台 ESXI 资源占用过高时，会将此服务器上的虚拟机自动漂移到资源占用相对较低的 ESXI 上，而 SVM 是不可以进行漂移的否则该 ESXI 服务器上的虚拟机将失去保护功能，故我们需要通过 VMware vSphere Client 或 web Client 登录 vCenter 中禁用 SVM 的 DRS 功能。

右键选择主机所在群集-编辑设置-选择虚拟机选项-找到 SVM 后选择禁用





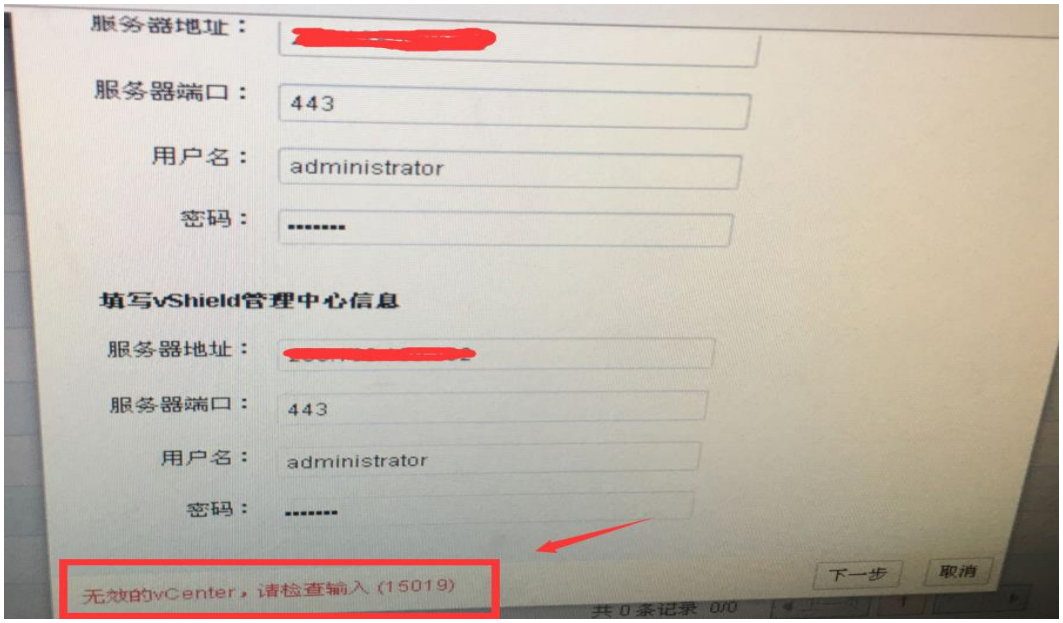
7. SVM 在 PMC 中被识别为虚拟机，导致安全防护失效？

该问题一般在正常参照产品使用手册部署的情况下，均是由于以下两方面造成：

- PMC 管理中心 GVM 操作系统默认开启的防火墙功能，导致 SVM 无法与 PMC 正常通讯，关闭系统默认防火墙或第三方防火墙。
- SVM 设置的 PMC 管理中心地址不正确，请重新设置 SVM 中的 Management Center 指向

的 PMC 管理中心地址，并在重启 SVM 后，重新刷新 PMC 页面或重新导入 Vcenter（详细设置说明请查看产品使用手册）。

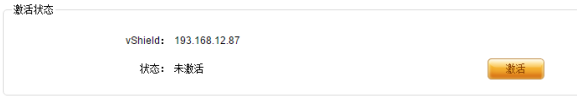
8. PMC 导入 vCenter 提示无效的 vCenter,请检查输入（15019）？



该问题需要按照如下步骤详细检查后基本均可解决：

- 再次确认在 PMC 中填写的 vCenter 和 vShield 管理中心用户名、端口、密码是否正确。
- 安装有 PMC 的机器网络是否可以与 vCenter 和 vShield 正常通讯，可以尝试在 PMC 系统本地浏览器登录以上两个平台看看是否正常。
- 如果所安装的 vCenter 在 5.5 版本或以上，而恰巧 PMC 安装在了 Windows 2003 的系统上，那么很不幸 VMware vCenter5.5 版本或以上，默认采用 SSL 的强密码套件，而 Windows XP 和 Windows 2003 均不支持，所以必然会导致 PMC 导入 vCenter 失败。当然微软也推出了针对该问题的操作系统热补丁文件，但目前 VMware 官网提供的补丁文件均针对英文版系统，在中文系统上无法正常安装，具体请查看 Vmware 官网发行说明（https://www.vmware.com/support/vsphere5/doc/vsphere-esx-vcenter-server-55-release-notes.html），故如果是此问题导致建议更换操作系统为 windows 2003 以上版本处理。

9. SVM 的 vShield 无法正常激活



此类问题（忽略报错的信息提示）主要是由于 SVM 与 vShield 之间通讯导致，主要排查一下几个方面：

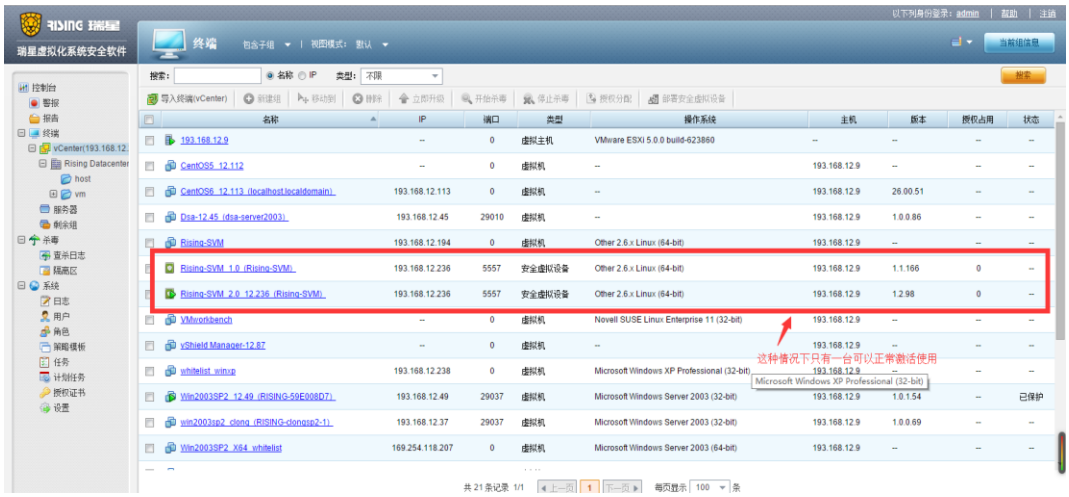
- 首先确认 vShield manager 许可授权是否已经过期，可通过登录 VMware vSphere Client 或 WEB Client 查看【许可】。

  PS: vmware vShield manager 许可授权在 vmware vsphere 5.1 版本或以下为独立许可授权序列号。而 vmware vsphere 5.1 以上版本均集成到平台基础序列号许可授权中，具体如果不清楚请咨询 vmware 厂商人员。

- 登录 vmware vShield manager 管理控制台，查看无法激活的 SVM 所在主机的 endpoint 是否正常，如发现相关异常情况，请咨询 vmware 厂商处理。

- 如果 vShield endpoint 状态正常，请登录 vCenter 查看 SVM 主机的网卡是否有 vmservice-vshield-pg 网卡，如果没有请手动添加。

- 一台 ESXI 上只允许部署 1 台 SVM，如果部署多台 SVM，则只有一台 SVM 可以成功激活，另一台必定激活失败，请通过 vCenter 或 PMC 查看无法激活的 SVM 是否所属主机是否存在多个 SVM 安全虚拟设备。



- ***还存在一种情况会导致无法激活 SVM 的情况，就是在未取消 SVM 与 vShield 激活状态的前提下，直接将 SVM 删除后重装了，这样必然会导致再次部署 SVM 后 vShield 状态无法激活，故务必请注意如因为异常状态需要重装 SVM 的情况下，请一定要先通过 PMC 把现有的 SVM 的 vShield 激活状态取消掉，否则如遇到此类问题，只能重装 vmware vShield manager 才可解决无法激活 SVM 的情况。***

10.PMC 客户端状态总是显示离线或未安装代理，是否就说明客户端没有被保护？

此问题是由于 GVM 内未安装查杀协作组件引起，查杀协作组件主要实现的功能是为了向 PMC 汇报 GVM 在线或离线状态、GVM 本地杀毒后弹泡提示、记录本地查杀日记以及自动恢复隔离文件的功能，与 GVM 是否已经被 SVM 防护并无直接关系。

查杀 GVM 是否已经被保护，请通过 PMC 客户端列表查看状态即可。

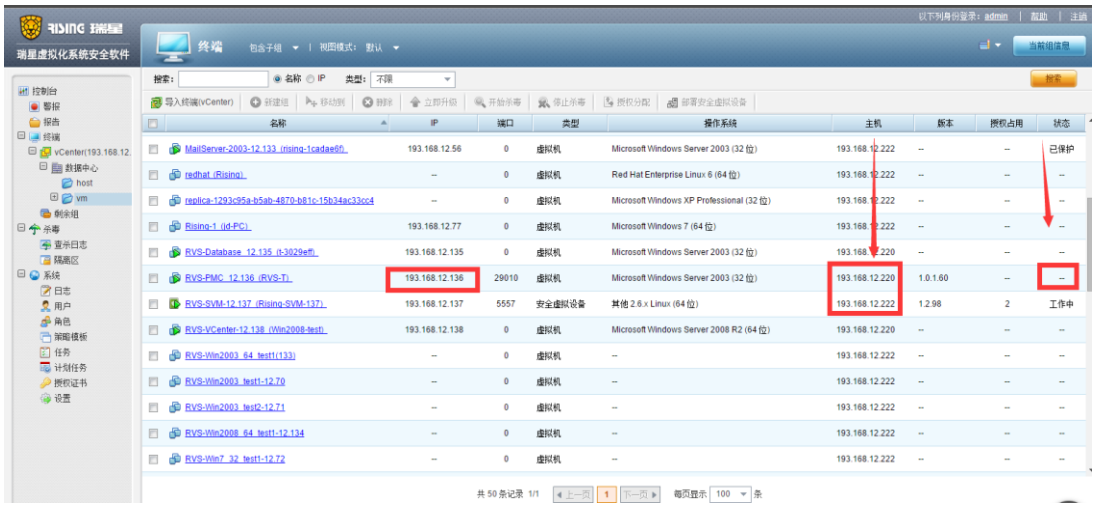
PS：从 SVM 版本 1.0.1.59 开始，PMC 上显示 GVM 的状态如果在没有安装查杀协作的情况下不再显示离线，修改为未安装代理。

旧版　　新版

11.客户端查杀一直处于等待状态，最后发现超时了？

一般遇到此类情况优先建议耐心等待，因为有可能是由于此前有相关查杀任务未完成，如果发现很长时间（2 小时以上）还是此状态，并最终状态返回为超时，请按照下面步骤详细检查。

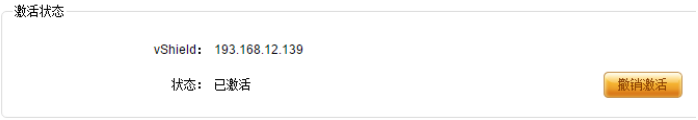
遇到此类情况优先检查确认，该任务查杀的客户端状态是否为已保护



如果是未保护状态请详细核实一下情况：

- PMC 管理页面-系统-授权证书，查看确认 PMC 中存在授权证书是否已经到期；
- PMC 管理列表中点击 SVM，查看确认 SVM 是否已经授权杀毒功能

- PMC 管理列表中点击 SVM ， vShield 状态是否已激活。



- PMC 管理列表中还需要检查 GVM 所在的主机上是否存在 SVM 或是否 GVM 所在主机内存在了多个 SVM，均会导致此问题，请正确调整后重新刷新浏览器再次查看状态。

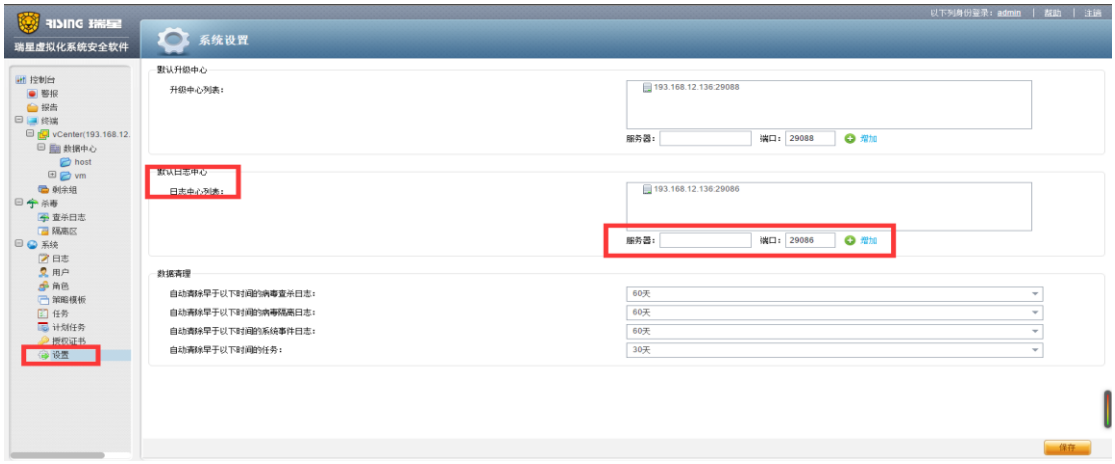
PS：具体安装部署方式请参考使用手册

12.客户端查杀一直处于排队中状态？

此问题一般均是由于存在多个查杀目标导致，请查看所执行的任务详情内，是否有多个查杀目标正在执行中，此状态请耐心等待即可。

13.客户端查杀扫描的文件数为 0？

此问题均是由于 PMC 管理中心未正确配置日志中心参数导致，请通过 PMC 平台点击设置-正确添加安装是配置的日志中心 IP 后，重新执行查杀即可。

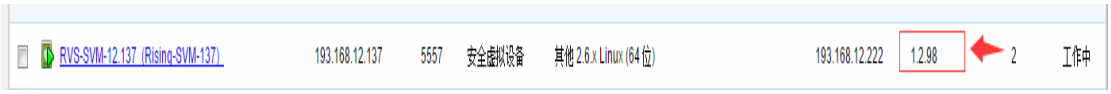


14.客户端二次查杀扫描的文件数为 0？

该问题目前已解决，请升级 SVM 版本至 1.0.1.50 版本以上即可。

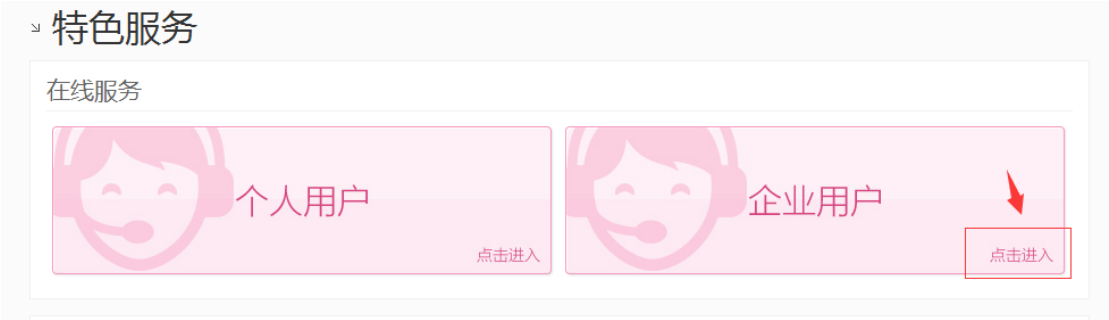
15.疑似病毒文件不报毒或病毒查杀失败？

此类问题优先确认瑞星虚拟化的 SVM 产品是否为最新版本。使用服务号登陆瑞星虚拟化自助平台查看当前 SVM 升级包版本



如升级为最新版本的 SVM 查杀后问题依旧，（如何升级 SVM 请参看使用手册），请务必尽快将相关疑似病毒或杀毒失败的病毒样本，通过瑞星客服在线服务平台渠道或致电客户服务中心的渠道反馈给我们。需要告知客服人员具体的 SVM 版本号和 PMC 版本。

- 瑞星客户服务电话：400-660-8866 （北京及未开通 400 电话地区：010-82678800）
- 瑞星客服在线服务平台地址：http://csc.rising.com.cn/index.html



16.PMC 为什么没有上报事件日志？

- 并不是所有任务及事件都会上传事件日志，例如：定时任务，计划任务都是不会上传事件日志的
- 请核查出现问题的 GVM 或者 SVM 的日志中心配置是否正确？
- 请核查日志中心中 IIS 的配置是否正确？例如 IP，端口等信息，不要只看日志中心的托盘设置，还要看系统 IIS 的配置。
- 检查 SVM 的网络是否可以与 PMC 联通。

17.PMC 为什么没有上报查杀日志？

- 检查 GVM，PMC，SVM 之间的网络通信。
- 确认病毒是否真的被查杀了？
- 如果病毒文件没有被查杀（按照问题 5 检查 SVM 没工作状态是否正常）
- 确认日志中心设置正确。

18.为什么 PMC 中事件日志中显示 12 点的时候有升级任务？

出厂默认设置的策略中有每天 12 点进行定时升级，请查看对应 PMC 的升级策略设置

19.操作 PMC 时，感觉 PMC 响应很卡？

出现这种情况优先查看安装 PMC 的机器，查看进程资源使用率，这种问题通常是因为 CPU 使用爆表了，请关注 interupts 以及无 w3wp.exe 这两个进程，如果是的话，说明 IIS 目前很忙，可尝试继续等待或重启虚拟机操作系统。

另外强烈推荐使用 google chrome 或火狐浏览器，以便保证控制台兼容性，此外不可使用低于 IE8 以下的 IE 浏览器。

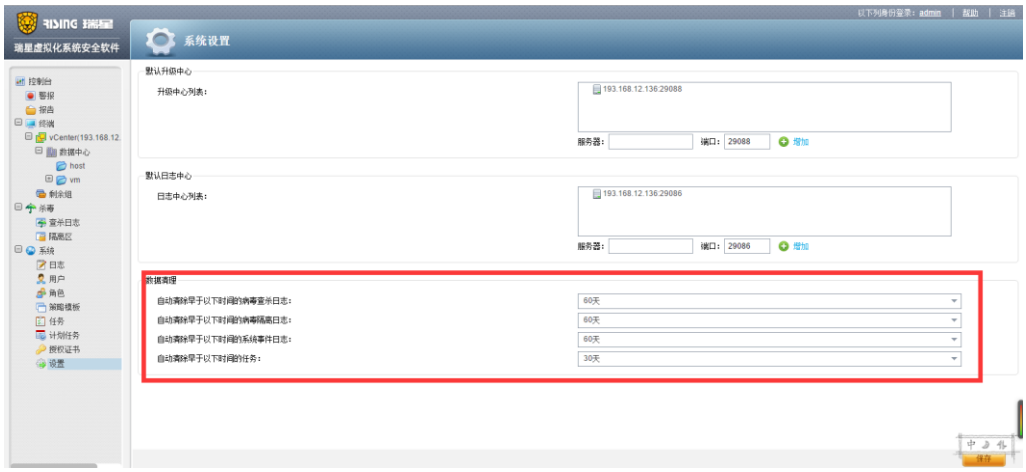
20.自动恢复隔离文件后，任务显示成功，但是目标路径下没有文件？

出现这种情况可能是因为自动恢复隔离文件的 GVM 没有关闭文件监控，从而造成恢复的文件被二次查杀，请通过 PMC 关闭 GVM 实时监控以便于恢复自动恢复隔离文件。

PS：此功能需要 GVM 安装查杀协作组件。

21.PMC 中的历史记录没了？

PMC 中有日志定时清理功能，默认保存 60 天日志，请自行查看设置的自动清理时间。



北京瑞星信息技术股份有限公司

2015 年 12 月 3 日