XXX 公司

Deep Security 测试报告

目录

1. 文档说明

本文档用于说明趋势科技为 XXX 公司提供的虚拟层防护解决方案，经过用户环境测试后的有效性验证。内容包括：

- **测试环境说明**

  说明此次测试环境相关组件以及环境搭建过程

- **防病毒功能测试**

  说明此次测试验证过程以及测试结果

- **防火墙功能测试**

  说明此次测试验证过程以及测试结果

- **虚拟补丁功能测试**

  说明此次测试验证过程以及测试结果

- **完整性监控功能测试**

  说明此次测试验证过程以及测试结果

本文档相关截图、日志、数据皆来源于此次实际测试环境，所有测试项目都达到了预计测试效果，达到测试目的。

2. 测试环境需求说明

DSM 控制台需求

程序	操作系统	功能
DSM	Win2008 sp2 64 位	DS 管理控制台 *至少分配 8GB 内存 *至少分配 2 颗志强 CPU
SQL2008	Win2008 sp2 64 位	存储日志 *至少分配 8GB 内存 *至少分配 2 颗志强 CPU

DSVA 客户端需求

DS 客户端安装是在每台物理机上以 DSVA 方式存在，安装方式与物理机增加无关，单台物理机上虚拟机数增加，相对应分配给 DSVA 的资源要增加，安装过程中，物理主机会重启，如下图所示

通讯需求

IP 地址需求：

1、DSM（SQL Server2008）、vShield Manager（VSM）各需要一个 IP 地址

2、每个 DSVA 需要一个 IP 地址

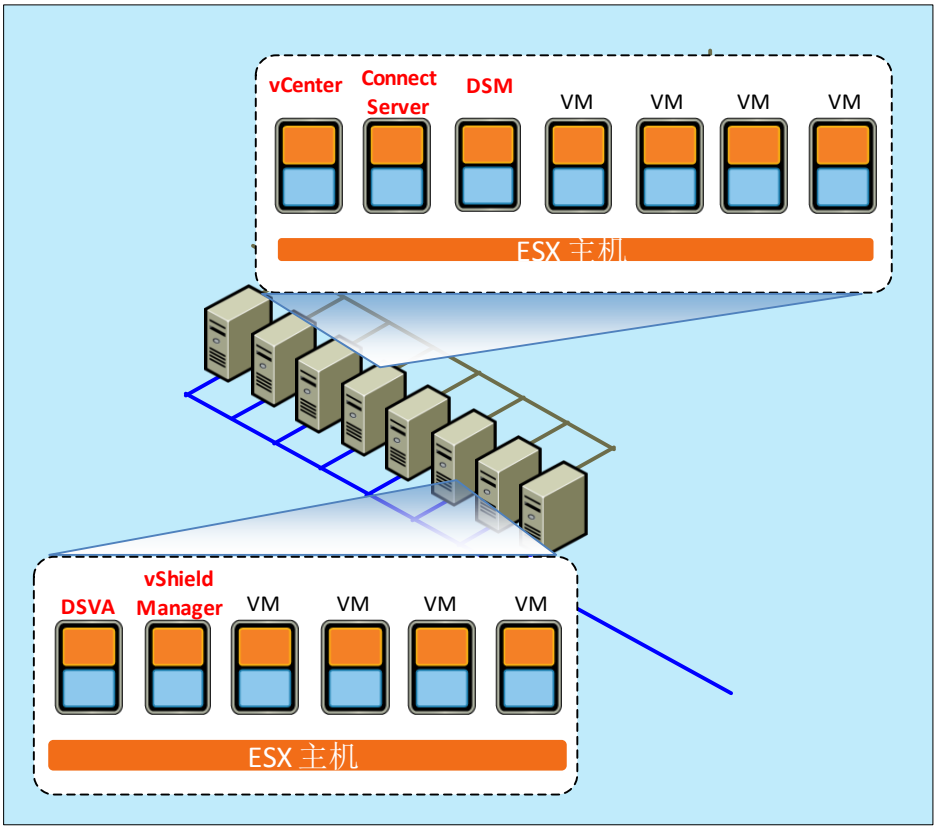
各组件访问规则需求：

序	源机器描述	目的机器描述	访问端口	备 注
1	DSM	VC	Tcp4119	双向
			Tcp443	
2	VSM	VC	Tcp443	双向
3	DSM	DSVA	Tcp 4118	双向
			Tcp 4120	
			Tcp 4122	
4	DSM	VSM	Tcp 443	双向
5	VSM	DSVA	Tcp 443	双向
6	DSM	Esx	Tcp 443	双向
			Tcp 4119	
7	VSM	Esx	Tcp443	双向

3. 测试环境说明

角色	IP 地址	web 控制台登录地址	系统类型	web 控制台用户名/密码	系统登录名和密码
DSM（Deep Secrutiy 控制端）	10.100.60.121	https://10.100.60.121:4119	windows 2008	masteradmin/masteradmin	administrator/-
ESX1	10.100.61.111	n/a	linux x64	n/a	n/a
ESX2	10.100.61.113	n/a	linux x64	n/a	n/a
ESX3	10.100.61.114	n/a	linux x64	n/a	n/a
ESX4	10.100.61.115	n/a	linux x64	n/a	n/a
vCenter	10.100.60.110	使用 vSphere Client 登录	windows 2008	administrator/-	administrator/-
vShield Manager（vmware 组件，用于完成底层防病毒）	10.100.60.122	https://10.100.60.122	linux x64	admin/default	admin/default
DSVA for ESX1（Deep Security 组件之一）	10.100.60.123	n/a	linux x64	n/a	dsva/dsva
DSVA for ESX2（Deep Security 组件之一）	10.100.60.124	n/a	linux x64	n/a	dsva/dsva
DSVA for ESX3（Deep Security 组件之一）	10.100.60.125	n/a	linux x64	n/a	dsva/dsva
Test-Machine-1 (Transfer Server)	10.100.61.167	n/a	windows 2008	n/a	administrator/-

注：其中为趋势 Deep Security 相关服务器
vmware 相关服务器
测试用虚拟机



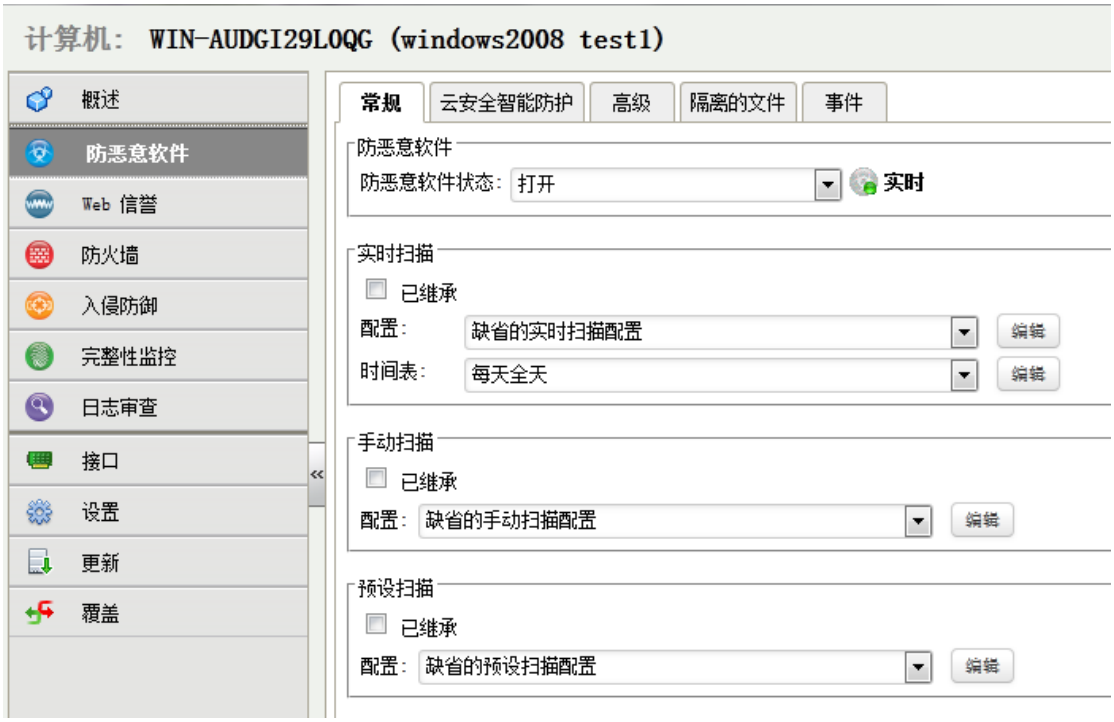
项目	测试环境搭建		
时间	2014/3/27		
步骤	描述	结果	备注
1.部署 vShield Manager	该步骤用户完成 vShield API 安装，以便完成稍后的底层无代理防病毒功能	□成功	
2.部署 Deep Security Manager	该步骤用于完成 Deep Security Manager	□成功	
3.部署 Deep Security Virtual Appliance	该步骤用于完成 vShield API 与趋势科技 Deep Security Virtual Appliance 联动	□成功	

4. 防病毒功能测试

趋势科技通过 Vmware 提供的 vShield API，无需在 Guest Server 安装客户端程序，即可实现免客户端的底层防护功能，实现基于实时/手动的病毒查杀功能。

1. 底层防病毒功能激活

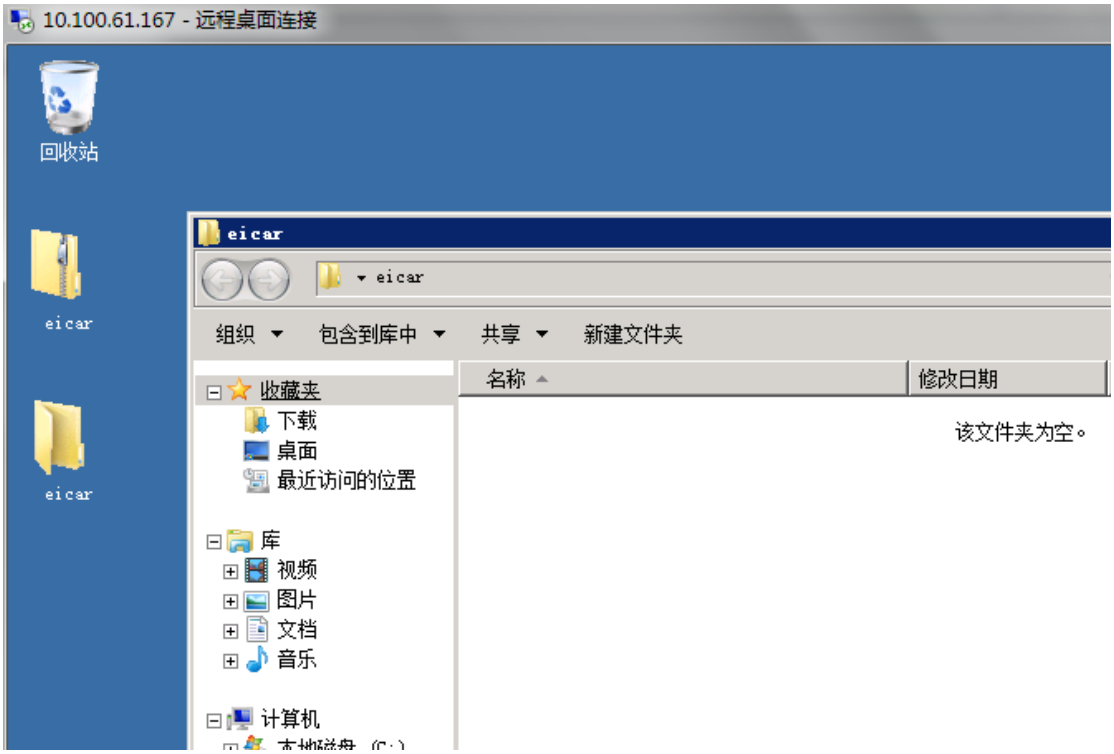
选取一台虚拟机，激活底层防病毒功能



2. 实时扫描功能测试

通过该虚拟机的解压下载的 eicar.zip 测试文件，实时扫描功能检测并处理位于读写状态中的 EICAR 测试病毒，该测试文件的解压缩过程被实时阻止并生成相关日志。

测试文件解压缩失败。



检测日志，在防恶意软件事件中发现解压缩的文件已经被隔离。

3. 测试结果

项目	虚拟层无客户端防病毒功能测试(针对 Win2008)		
时间	2014/3/27		
步骤	描述	结果	备注
1.激活实时扫描功能，将测试病毒 Eicar 释放到本地硬盘；正常情况下，该文件无法释放，DSM 上可观察到相关文件被隔离的日志	该步骤用于验证趋势科技解决方案可以实时地对来自外部的病毒进行处理	□成功	无
2.以上步骤执行过程中，无兼容性问题	该步骤用于验证趋势科技解决方案在运行中不会对用户环境产生兼容性问题	□成功	
3.以上步骤执行过程中，无性能问题	该步骤用于验证趋势科技解决方案在运行中不会对用户环境产生性能问题	□成功	

5. 防火墙功能测试

趋势科技通过 Vmware 提供的 vSafe API，无需在 Guest Server 安装客户端程序，即可实现免客户端的底层防护功能，实现基于流量内容的虚拟补丁功能，实现过滤针对利用操作系统漏洞进行攻击的流量。

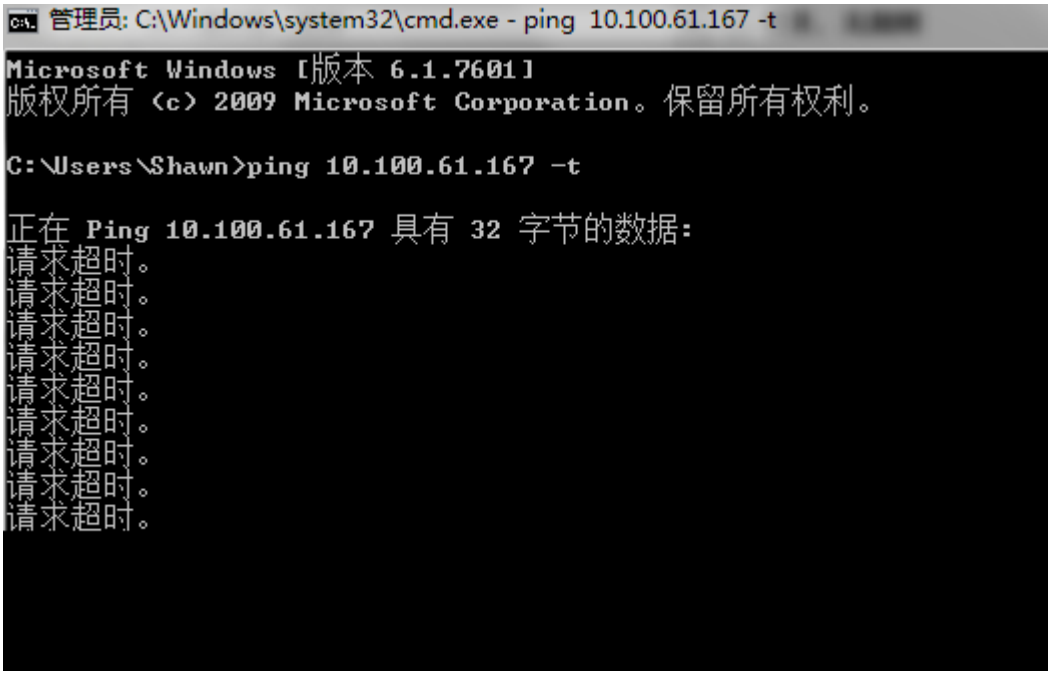
1. 搭建用于测试的环境

进入测试策略界面开启防火墙功能

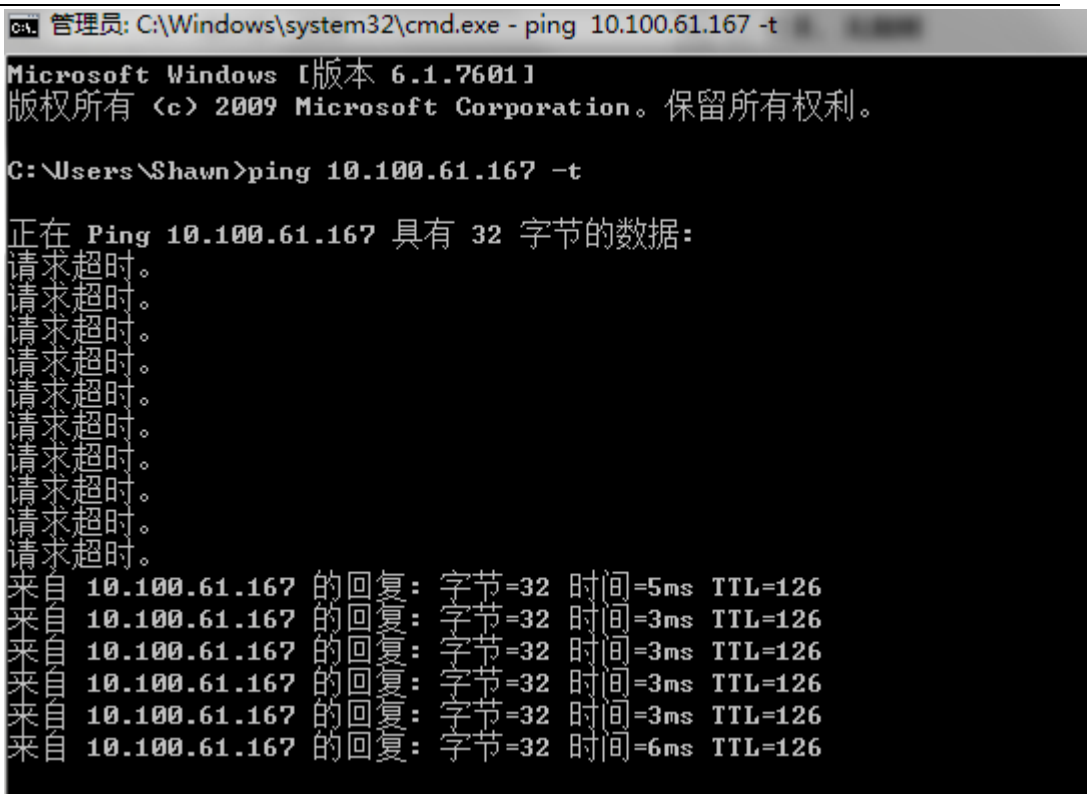
建立一条策略，禁止 icmp 包传入

启用策略

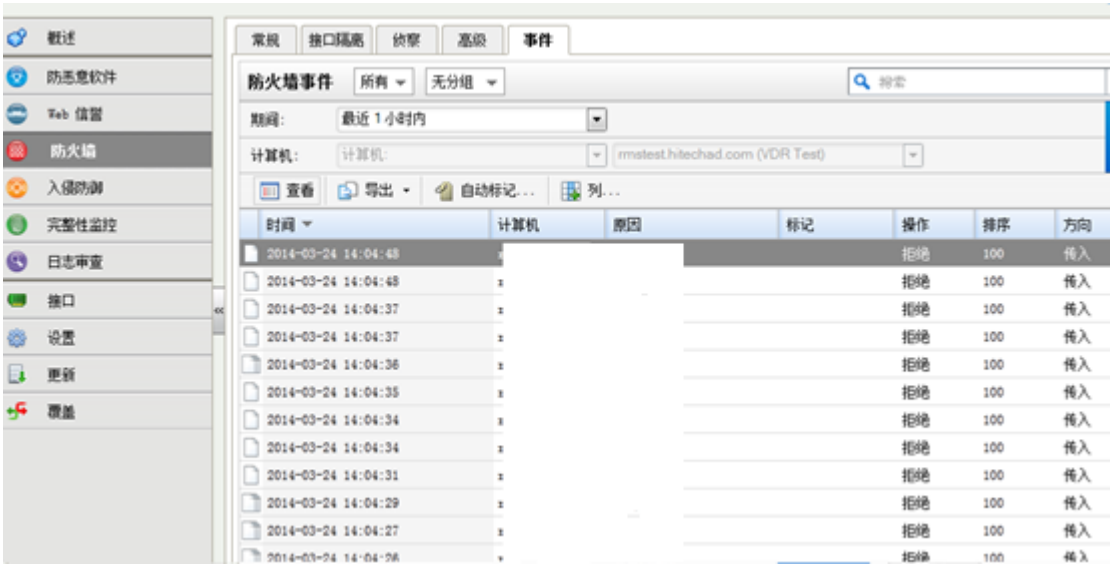
使用 ping 命令测试策略是否生效，策略已经生效



同时关闭策略


管理员: C:\Windows\system32\cmd.exe - ping 10.100.61.167 -t
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\Shawn>ping 10.100.61.167 -t
正在 Ping 10.100.61.167 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
来自 10.100.61.167 的回复: 字节=32 时间=5ms TTL=126
来自 10.100.61.167 的回复: 字节=32 时间=3ms TTL=126
来自 10.100.61.167 的回复: 字节=32 时间=3ms TTL=126
来自 10.100.61.167 的回复: 字节=32 时间=3ms TTL=126
来自 10.100.61.167 的回复: 字节=32 时间=3ms TTL=126
来自 10.100.61.167 的回复: 字节=32 时间=6ms TTL=126

检测事件记录


概述
防恶意软件
Web 信誉
防火墙
入侵防御
完整性监控
日志审查
接口
设置
更新
覆盖
常规
接口隔离
侦察
高级
事件
防火墙事件
所有
无分组
期间:
最近 1 小时内
计算机:
查看
导出
自动标记...
列...
时间
计算机
原因
标记
操作
排序
方向

2. 测试结果

项目	虚拟层无客户端防火墙功能测试(针对 Win2008)		
时间	2014/3/27		
步骤	描述	结果	备注
1.激活防火墙功能；可通过虚拟机状态以及 system event 查看是否设置	该步骤用于启用防火墙防护功能，为后续测试做准备		无
2.在测试 VM 上部署 icmp 禁止传入测试，启用策略	该步骤用于测试防火墙功能针对协议和包的有效性		
3.使用 ping 命令验证策略部署	该步骤用于确认防火墙策略是否正确生效，有效拒绝 icmp		
4.在测试 VM 上关闭部署的 icmp 拒绝策略	该步骤用于对策略的二次验证		
5.继续使用 ping 命令验证策略是否生效	该步骤用于确实防火墙策略取消后 icmp 包的传输是否正常		
6.以上步骤执行过程中，无兼容性问题	该步骤用于验证趋势科技解决方案在运行中不会对用户环境产生兼容性问题		
7.以上步骤执行过程中，无性能问题	该步骤用于验证趋势科技解决方案在运行中不会对用户环境产生性能问题		

6. 深度包检测功能测试

趋势科技通过 Vmware 提供的 vSafe API，无需在 Guest Server 安装客户端程序，即可实现免客户端的底层防护功能，实现基于流量内容的虚拟补丁功能，实现过滤针对利用操作系统漏洞进行攻击的流量。

1. 测试工具说明

A). DemoSQL 为模拟 SQL Slammer 攻击行为的演示工具（并不会对操作系统产生实际影响），利用 Microsoft MS02-039 相关漏洞。

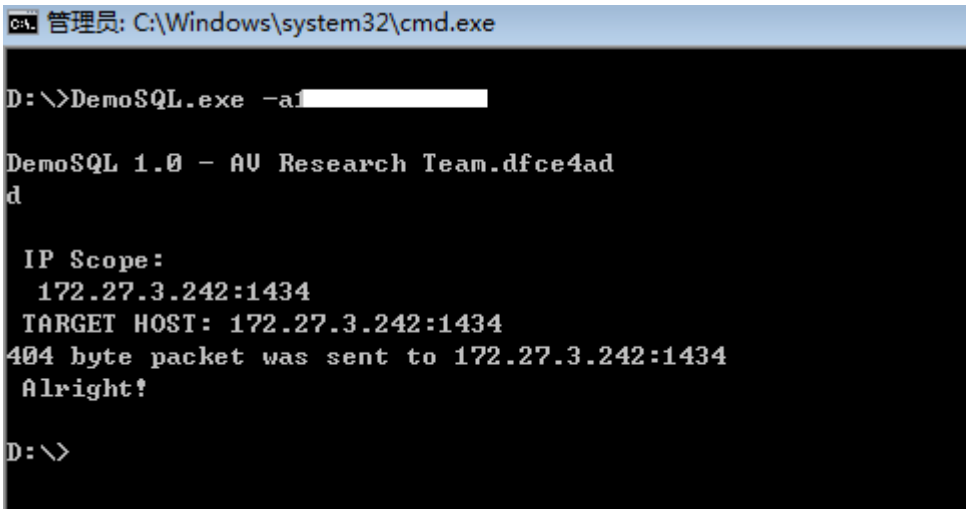
B). lesssecurity.py 为模拟针对远程桌面协定重大漏洞攻击行为的演示（会对操作系统产生实际影响，不建议在生产环境中测试），利用 Microsoft MS12-020 相关漏洞。

2. 测试一：

激活虚拟补丁防护策略

启用 DPI 策略”1000617: MS-SQL Slammer Worm”

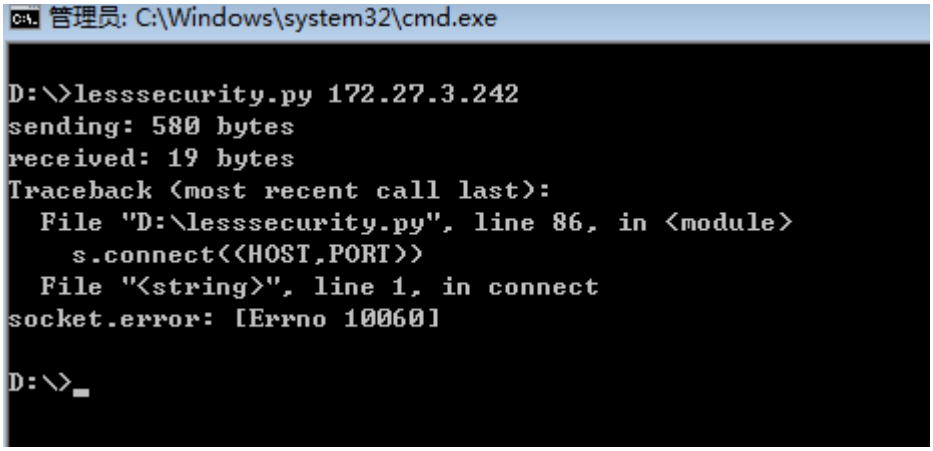
使用 DemoSQL 工具进行模拟攻击



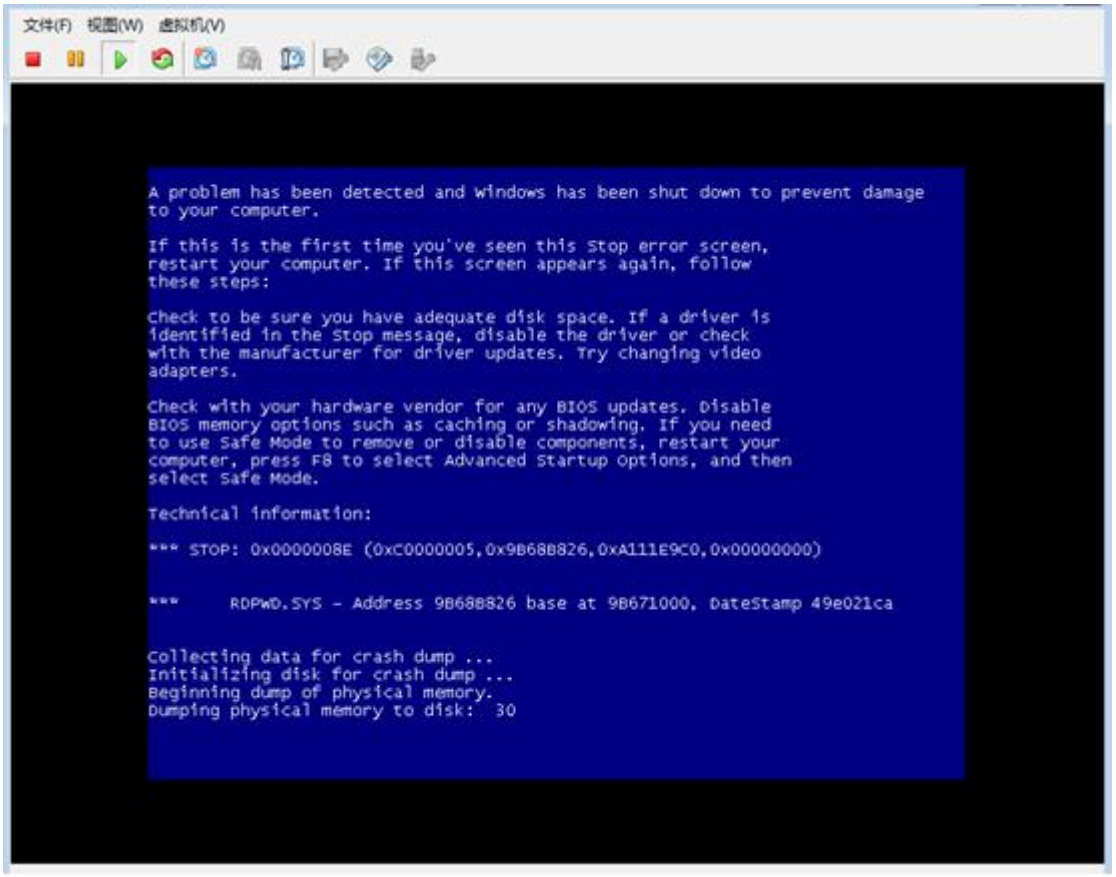
查看相关 DPI 日志

3. 测试二

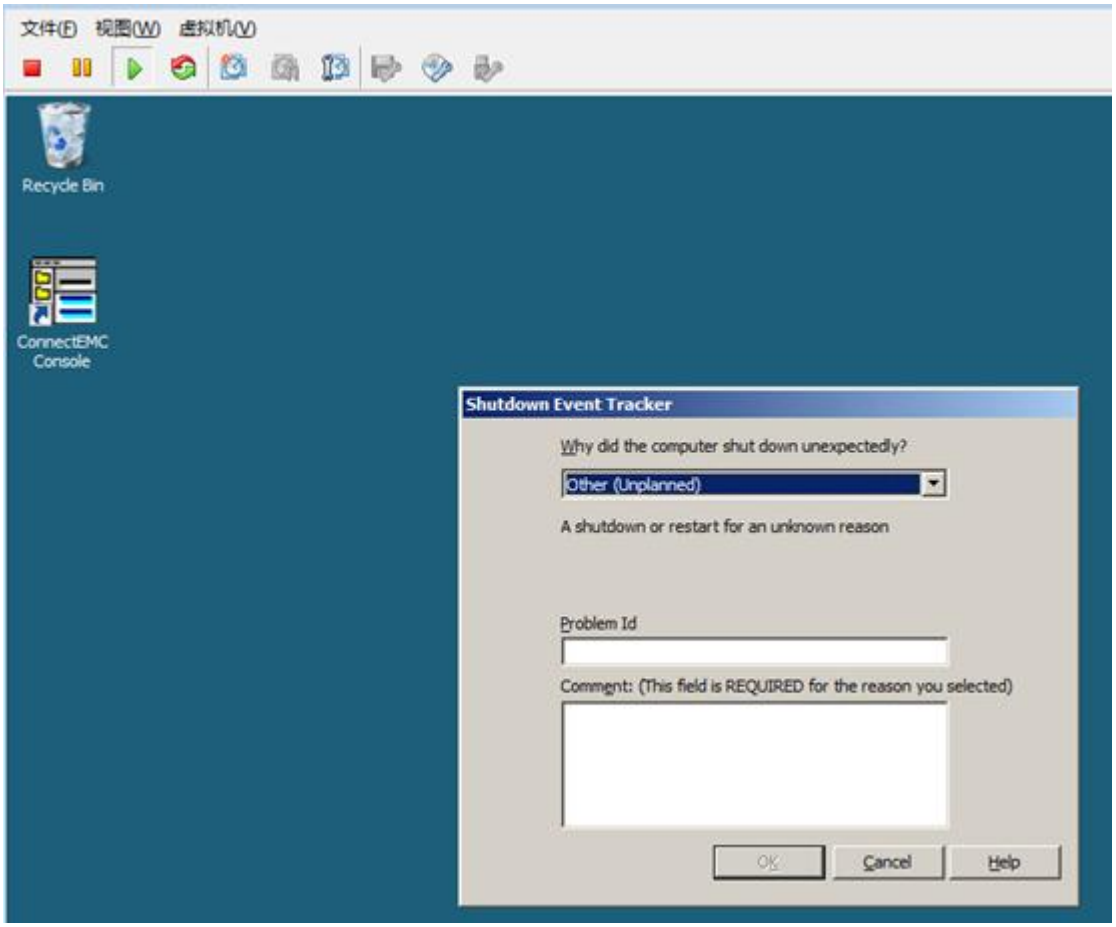
未应用虚拟补丁防护策略测试攻击



攻击成功，被攻击主机蓝屏


文件(F) 视图(W) 虚拟机(V)
A problem has been detected and Windows has been shut down to prevent damage
to your computer.
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.
Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x0000008E (0xC0000005,0x9B688826,0xA111E9C0,0x00000000)
*** RDPWD.SYS - Address 9B688826 base at 9B671000, DateStamp 49e021ca
Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 30

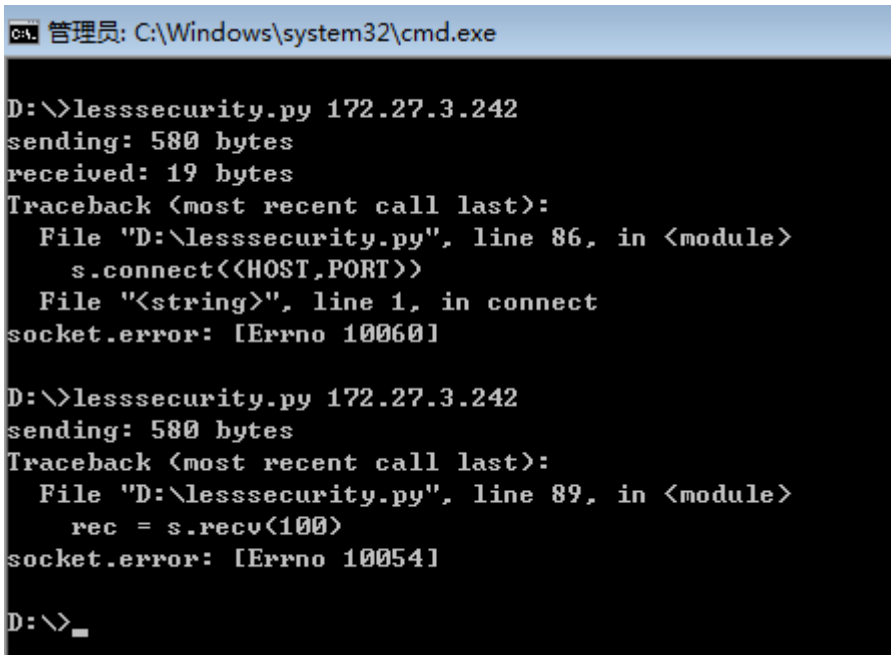
主机重启，错误信息



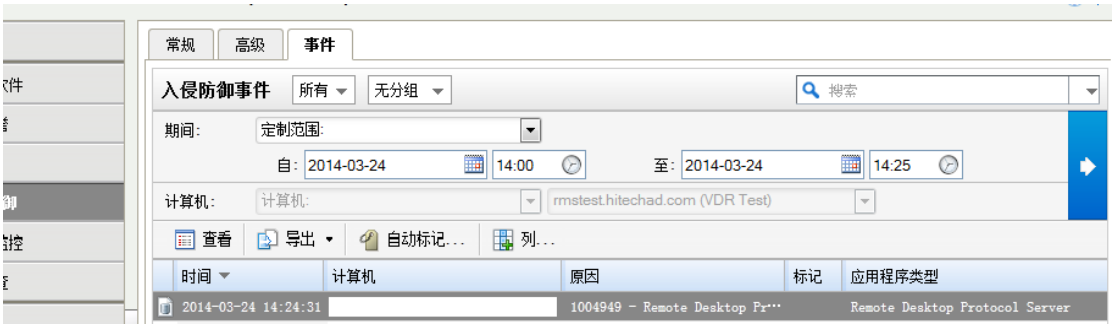
激活虚拟补丁防护策略

启用 DPI 策略”1004949 – Remote Desktop Protocol Vulnerability (VCE-2012-0002)”

攻击失败，主机未出现蓝屏


管理员: C:\Windows\system32\cmd.exe
D:\>lesssecurity.py 172.27.3.242
sending: 580 bytes
received: 19 bytes
Traceback (most recent call last):
File "D:\lesssecurity.py", line 86, in <module>
s.connect((HOST,PORT))
File "<string>", line 1, in connect
socket.error: [Errno 10060]
D:\>lesssecurity.py 172.27.3.242
sending: 580 bytes
Traceback (most recent call last):
File "D:\lesssecurity.py", line 89, in <module>
rec = s.recv(100)
socket.error: [Errno 10054]
D:\>

查看相关 **DPI** 日志


常规
高级
事件
入侵防御事件
所有
无分组
搜索
期间:
定制范围:
自:
2014-03-24
14:00
至:
2014-03-24
14:25
计算机:
计算机:
rmstest.hitechad.com (VDR Test)
查看
导出
自动标记...
列...
时间
计算机
原因
标记
应用程序类型
2014-03-24 14:24:31
1004949 - Remote Desktop Pr...
Remote Desktop Protocol Server

4. 测试结果

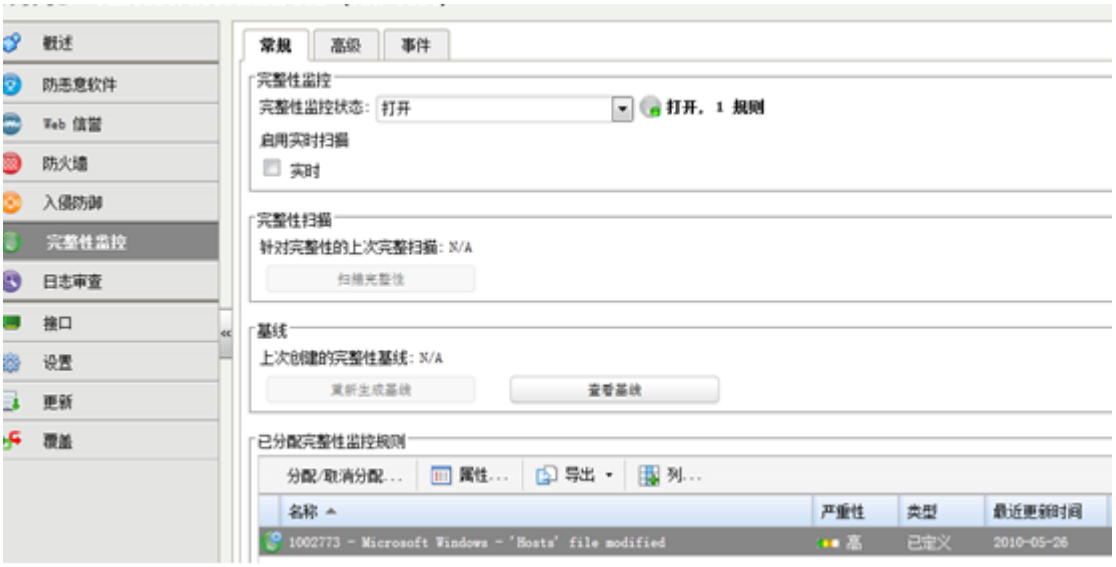
项目	虚拟层无客户端防火墙功能测试(针对 Win2008)		
时间	2014/3/27		
步骤	描述	结果	备注
1.激活 DPI 功能；可通过对应虚拟机状态以及 system event 查看是否设置成功	该步骤用于启用 DPI 防护功能，为后续测试虚拟补丁做准备	□成功	无
2.使用 DPI 虚拟补丁策略，屏蔽 SQL 演示攻击；正常情况下，可以通过 DPI Event 查看是否防护成功	该步骤用于确认 DPI 虚拟补丁策略正确生效，有效屏蔽基于 Microsoft MS02-039 攻击	□成功	
2.使用 DPI 虚拟补丁策略，屏蔽利用远程桌面协定漏洞的演示攻击；正常情况下，可以通过 DPI Event 查看是否防护成功	该步骤用于确认 DPI 虚拟补丁策略正确生效，有效屏蔽基于 Microsoft MS12-020 攻击	□成功	

7. 完整性监控

趋势科技通过 Vmware 提供的 vSafe API，无需在 Guest Server 安装客户端程序，即可实现免客户端的底层防护功能，实现基于注册表/系统文件状态检测的完成性监控功能。

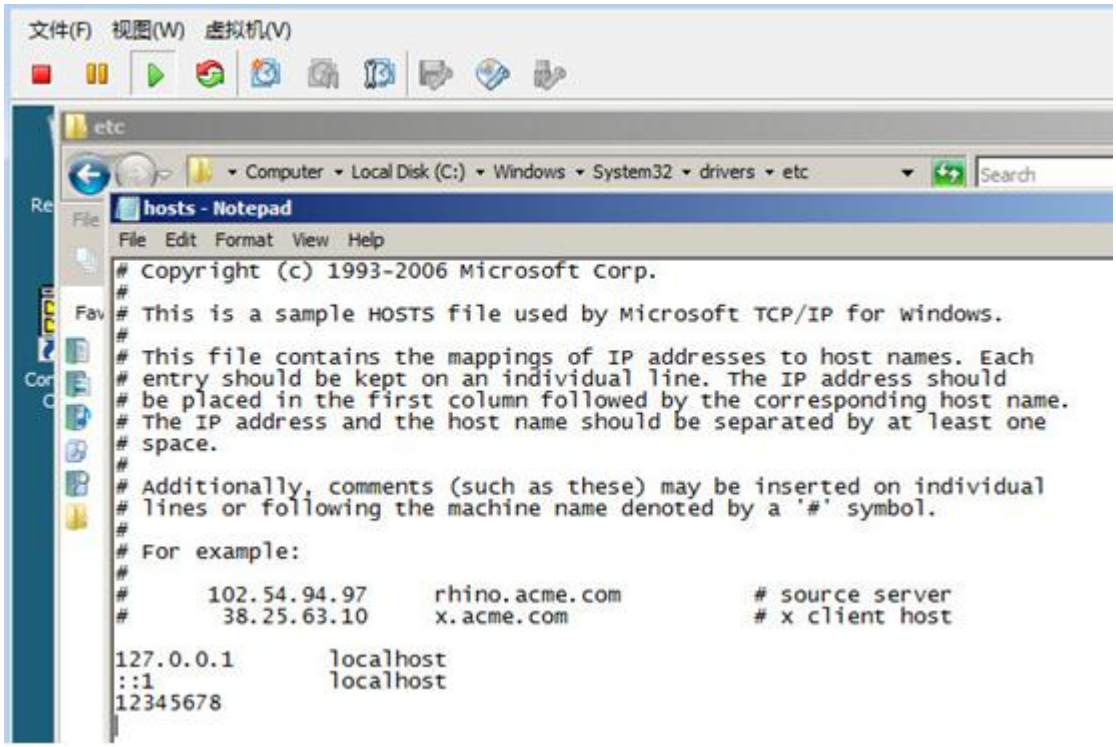
1. 搭建用于测试的环境

进入测试策略管理界面开启完整性监控功能

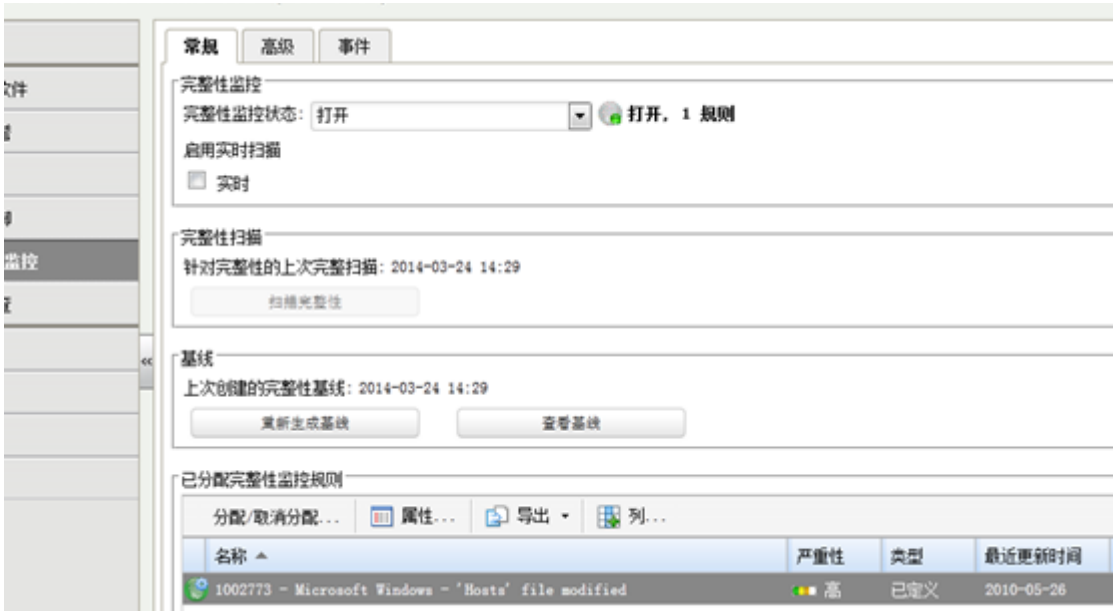


2. 开启监控 hosts 文件的策略，扫描生成基线

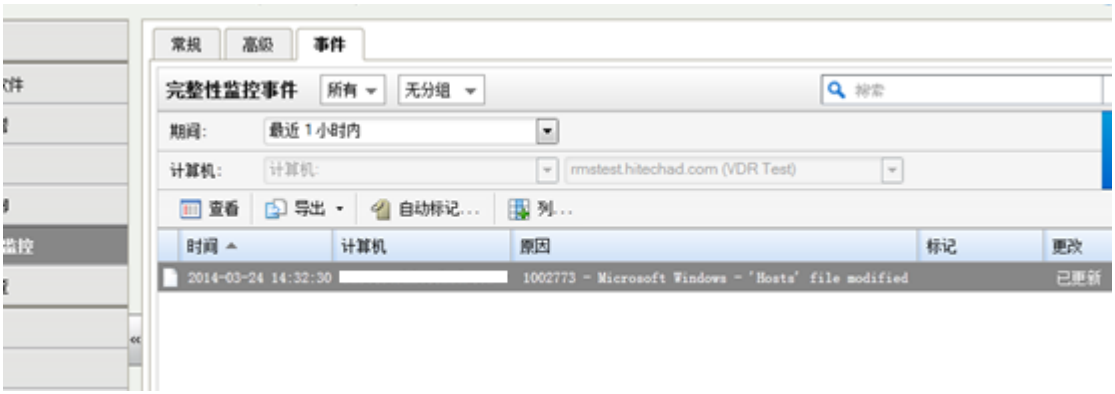
3. 修改测试机的 hosts 文件



4. 扫描此时测试机的完整性，同时生成基准线



5. 事件预警



6. 测试结果

项目	虚拟层无客户端完整性监控功能测试(针对 Win2008)		
时间	2014/3/27		
步骤	描述	结果	备注
1.激活完整性监控功能可以通过针对测试机生成完整性基准线	该步骤用于启用 hosts 文件监控，生成测试系统的完整性基准线	成功	无
2.更改测试机器的 hosts 文件，出发完整性监控策略的实时性	该步骤用于触发部署的完整监控策略，并且以事件的形式发出通知	成功	