#### 客户端实用工具

天珣客户端诊断工具	2
天珣服务器诊断工具	3
客户端卸载工具	4
Winmd5Hash.exe	5
离线同步工具	7
Radius By Pass 工具	14
Radius 故障告警工具	15

天珣自带有部分供服务器和客户端使用的工具,包括服务器诊断工具、客户端诊断工具 离线补丁工具等,这些工具放在安装光盘的 tools 目录中。

#### 天珣客户端诊断工具

天珣客户端诊断工具是当客户端发生异常,例如线程、句柄数过多,CPU、内存占用率 过高,CC无法停止服务等,收集客户端软硬件信息以及 dmp 文件以便分析的一个实用诊断 工具。

在客户端发生异常而无法定位时,管理员将天珣客户端诊断工具拷贝到客户端任何一个 目录里,运行:

(作名) 明月(1) 王首(1) 作用(1) 三月(1) 新	Rhall	11	
) AU • 🔘 👔 🔎 MR 🐑 ZHA			
Migil (⇔c)X		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
ALLES S POLICE D. MARSHARDER D. MARSHARDER P. MARSHARDER P. MARSHARDER P. MARSHARDER D. MILLER D. MILLE	Loads Discurration and Settings ND DD VEROVE	Frogra Files	-
文件相互件未在各     《     》     和你忍证了文件     经码达订文件     经码达订文件     经码达订文件     经码达订文件     经码达订文件     经问户面件未过承述法     文件     和除这门文件     新闻之门文件	1244.554.588		
X:20 8			

运行后显示"正在收集信息中,请稍候。。"此时工具将收集必要的信息,完成后将自动 打开已收集信息的文件目录:

Collector		
文件化 编辑化 查得	(1) 收藏(1) 工具(1) 帮助(1)	27
😋 sa 🔹 🕤 👔	🏌 🔎 號家 🏀 文件夹 🔟 •	
Hill (1) 🙆 C: \Frigrie 7	iles/Venastech/Endpoint Security/ESOC/Cellector	🛩 💽 HI
文件和文件夹任务 ② 包建一个新文件共 ● 将这个文件共发和 ¥a3 二 其李此文件共	8) Date 2010-8-6_T2 2010-8-6_T2	έ <sub>.</sub> τι
大宅位置 - 5000 - 第8000時 - 日本総営	8	
计编辑系统	8	

默认文件保存在客户端安装目录的 collector 目录下,只有在运行过客户端诊断工具之后 才会自动产生此目录。

将此诊断文件进行分析,可以深层次的分析出客户端目前的运行状态,从而有针对性的 发现问题和解决问题。

## 天珣服务器诊断工具

天珣服务器诊断工具与客户端诊断工具类似,在服务器出现异常时,可以用此工具收集 一些必要的信息和 dmp 文件:

S新	小大	美型 修改日期	90.00		
二萬總計丁工具	C:Sfregram Files/Feau	ctech/Radpeint Security/RISe	ever Wellester		_101 ×
家户级的任工具	文件(12) 機構(12) 葺着(2)	·收藏(A) 工具(I) 帮助(A)			R.
天地服务器信纸	Q ALL - 0 - 7 PH	* 🚬 🗴 🕹 🗶 🖏	<b>m</b> -		
是天地客户南京街、	Hit (1) C: V2ragram Files	Wennatech/Endpaint Security/ESS	Garwar\Collactor		- 💽 神輿
	名称 -	大小 使型	修改員購	業性	Concerne of

运行完成后在服务器安装目录的 collector 目录下生成诊断文件,并由这个诊断文件来分析服务器出现的问题。

# 客户端卸载工具

虽然天珣提供自动卸载客户端的策略配置,但是有时由于某些未知原因,天珣客户端无 法卸载或者卸载不完全,此时可以使用此客户端卸载工具将客户端完全卸载掉。

沪端卸载 L具 exe	注意	×
	4 确定要卸	散客户端吗?
	是(1)	否例

在客户端上运行此卸载工具:

点击"是"进行卸载,完成后提示:

ノー Shap 単数 工具 exe		
	注意	
	客户端卸载成功,设	青重启计算机:

点击"确定"后将会显示卸载过程和删除与未删除的文件信息:

2件名	操作	1
<pre>iVEIDOOWS.ysystem32%lprind.dll :VEIDOOWS.ysystem32%lprind.dll :VEIDOOWS.ysystem32%lprind.aysettam32%lprind.ays :VEIDOOWS.ysystem32%lprind.aysettam32%lprind.aystem32%lprind.ay</pre>	●素素素素型工作学校不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不不	

系统重启后客户端就已完全卸载。

# Winmd5Hash.exe

此工具是用来对某些进程或文件生成 md5 码的,在配置进程红名单时,可能担心客户 端通过修改文件名等方式伪造红名单进程,那么可以通过对此进程或软件进行 md5 码校验 来避免。

	In the A IN CE	- 4- 44 +4 M )	
◎进程管理策略	红名里(必须)	运行的软件)	
O软件安装管理 OWindows服务管理	程序名称	Rtvscan. exe	程序名称不要包含完整路径, *只要后面的文件名加后缀
◎防病毒软件策略 ◎终端安全加固策略	程序描述	赛门铁克防病毒	
			*
□○共享资源管理 □○密码保护策略	下载此软件的网址		
● 准入控制	"或"操作程序组	不属于程序组	
→●女王的护 →●补丁管理 →●资产管理 →●非法外联	MD5校验码		
			>>
O桌面运维 O信息中心	在线模式	🔽 在线时生效 🔽 离线时生效	
O系统级联	应用到IP组	(还没有应用到任何IP组)查看及编辑	
◎更新策略	创建状态	全局	
●修改密码	创建者	administrator	
	は・古け右*早的価	目必须输入。	

此工具就是用来从外部生成 md5 码的, 双击打开工具:

🎒 TinED5Hash				
<u>文件 ?</u>				
┌选择类型 ───				
○ 字符串	⊙ 文件	〇 目录	□ 包含子目录	
MD5对象				
				浏览
计算	]			
MD5				复制MD5结果
[无MD5结果]				
└				
可以通过托放文	件图标到MD52	时象输入框选择文	C件	
复制MD5结果可	以将MD5值复制	制到剪贴板		

选择"文件"、"字符串"或"目录",以"文件"为例,点击浏览选择想要生成 md5 码 的文件或进程名:

🌐 TinED5Hash				
文件 ?				
┌选择类型 ────				
○ 字符串	◉ 文件	〇 目录	□ 包含子目录	
MD5对象				
ו Files\Venuste	ech\Endpoint	Security\ESServ	/er\ESServer.exe	浏览
计算				
结果				
MD5				复制MD5结果
1cb0c4123139	)d9bb61d894	e808fd5d37		
「堤不	u BRI+≓⊼ikan na		مهد الله	
可以通过托放艾德	于图标到MD5X	可象输入框选择了	21年	
复制MD5结果可以	以将MD5值复制	前到剪贴板		

点击计算即可生成 md5 码值,再点击"复制 md5 结果",将其复制到剪贴板,然后在 配置策略时将此 md5 码粘贴过去即可。

经过 md5 码校验的红名单进程或软件,如果客户端伪造一个同名称的进程,将会被检

测到与 md5 码不匹配导致客户端不符合安全基线要求。

#### 离线同步工具

在一些军工或政府部门,一般内网中是不允许上互联网的,但是用户可能又需要使用在 线补丁和更新病毒码的功能。由于无法上网中心服务器无法连接到互联网上的外网服务器, 那么只有通过离线同步工具来间接导入外网服务器上的补丁和病毒码。

"离线同步工具"位于 tools 文件夹中。当中心服务器不能连接外网时,就可以使用"离 线同步工具"去同步外网上的补丁。 "离线同步工具"需要有一个有效的 license 授权才能 去同步外网上的补丁,将离线同步工具和有效的 license 一起拷贝到能连接外网的计算机上, 便可下载外网上的补丁,并且会在离线同步工具目录下生成一个名为 OfflineHotfix 的文件 夹,所有从外网下载回来的补丁都放在该文件夹下。当同步完外网补丁之后,将离线同步工 具文件夹整个的拷贝到装有中心服务器的计算机上,"补丁导入本地"便可将 OfflineHotfix 文 件 夹 里 面 的 补 丁 文 件 全 部 导 入 到 中 心 服 务 器 Venustech\Endpoint Security\ESServer\Download\AutoUpdate 目录下。

注意 1: 运行离线同步工具的计算机必须安装 framework。

注意 2: 有效 license 授权是指没有过期的并且是天珣研发中心正式授予的 license,不受 IP 地址绑定的限制

**注意 3**:离线同步工具不支持断点续传,即如果在同步外网补丁中途断网的话,只能重新运行该工具。

**注意 4:** 离线同步工具只能将补丁导入中心服务器,不能导入到本地服务器,本地服务器上的补丁必须从中心服务器上同步。

注意 5: 离线同步工具同步外网服务器上的补丁文件时,该工具所在的目录盘的可用空间必须大于 2G

离线同步工具使用流程是这样的:

首先将离线同步工具拷贝到一台可以上互联网的普通 PC 上,通过这台能上互联网的 PC 将外网服务器的补丁和病毒码同步下来,然后再将这些补丁、病毒码和一些相关配置文件拷 贝到内网的中心服务器上进行导入即可。

离线同步工具导入外网补丁

将 license 放在离线同步工具目录下,并拷贝到可上互联网的机器上,点击运行 offlineDSrv,并点击"外网补丁下载":

副打开       共事       新聞       新聞       新聞       大小         ● 「下版       ● Advete fiskisked II       2009/4/37 1667       通用短序广超       00 x         ● Advete fiskisked II       2009/4/37 1667       通用短序广超       00 x         ● Advete fiskisked II       2009/4/37 1667       通用短序广超       00 x         ● Advete fiskisked II       2009/4/37 1067       通用短序广超       12 x         ● Advete fiskisked II       2009/4/37 1067       通用短序广超       12 x         ● Advete fiskisked II       2009/4/37 1067       通用短序广超       12 x         ● Advete fiskisked II       2009/4/37 1067       通用短序广超       12 x         ● Advete fiskisked II       2009/4/37 1067       通用短序广播       14 x         ● Manage dubis dI       2009/12/3 1158       通用短序广播       14 x         ● Advete fiskisked II       2008/7/23 1158       通用短序广播       14 x         ● DPDServiceClient dI       2008/7/23 1158       通用短序广播       16 x         ● Advete fiskisked II       2008/7/23 1158       通用短序作用       16 x         ● Advete fiskisked II       2008/7/23 1159       通用       16 x         ● Advete fiskisked II       2008/11/3 16 x       MRE       MRE         ● Advete fiskisked II       Advete fiskisked II       Advete fiskis	
● 下號       ▲ Advitefisilia.dll       2009/4/17 1607       屈用程序17월       00 x         ● 正式式可容的公式       ● Advitefisilia.dll       2009/4/17 1607       屈用程序17월       00 x         ● 正式式可容的公式       ● ConneonFunc.dll       2009/12/5 1007       Generation 2008/7/23 11:56       日用程序17월       241 x         ● 面片       ● ConneonFunc.dll       2008/7/23 11:56       日用程序17월       241 x         ● 面片       ● OfficeOSiv       2010/8/17 17:53       血用程序17월       241 x         ● OfficeOSiv       2008/7/23 11:58       血用程序       241 x         ● OfficeOSiv       2008/7/23 11:58       血用程序       24 x         ● OfficeOSiv       2008/7/23 11:58       血用程序       24 x         ● More       ● OfficeOSiv       2008/17/3 15:29       血用程序         ● Advitefision       ● Advitefision       Advitefision       Advitefision         ● Advitefi	●数目期         単型         大小           2009/4/17 16-07         但用程序扩置         80 K3           2010/8/17 17:14         Microsoft Office         576 K3           2009/12/5 10-07         位用程序扩置         241 K3           2009/12/5 10-07         位用程序扩置         241 K3           2009/12/5 10-07         位用程序扩置         241 K3           2009/12/5 10-07         位用程序扩置         244 K3           2008/7/23 11:58         位用程序扩置         84 K3           2008/11/3 16:29         应用程序扩置         116 K8           1         /所專码版本         /新南码版本         /新           小网病毒码版本下载         /病毒码版本导入到本地         /*
下載       ▲ Adv+tefiaLia.dli       2009/4/17 16-07       田田健野11種       00 x         ● Within 1000000000000000000000000000000000000	2009/4/37 16-07
<ul> <li>▲ 調 ● CenterDS ● CommonFunc.dll ● CommonFunc.dll</li></ul>	2010/8/37 17:14 Mereauth Office. 576 83 2009/12/5 10:07   血用程序扩展 241 83 2008/7/23 11:58   血用程序扩展 32 43 2008/7/23 11:58   血用程序扩展 84 68 2008/11/3 16:29   血用程序扩展 116 68 2009/11/3 16:29   血用程序扩展 116 68 2009/11/3 16:29   血用程序扩展 116 68 2009/11/3 16:29   血用程序扩展 116 68
<ul> <li>■ ####################################</li></ul>	2009/12/5 10:07 益用程序扩展 241 K3 2008/7/23 11:58 运用程序扩展 12 K8 2008/7/23 11:58 应用程序扩展 84 K8 2008/71/3 16:29 应用程序扩展 116 K8 2008/11/3 16:29 应用程序扩展 116 K8 1 // 病毒码版本下载 病毒码版本导入到本地
<ul> <li>■ ManagedUikdi 2008/7/23 11:50 应用程序扩送 32 ×</li> <li>● ManagedUikdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ dilineDSrv 2010/07/23 11:50 应用程序扩送 416 ×</li> <li>○ UPDServiceClientdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ UPDServiceClientdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ UPDServiceClientdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ ManagedUikdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ UPDServiceClientdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ ManagedUikdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ UPDServiceClientdi 2008/7/23 11:50 应用程序扩送 416 ×</li> <li>○ ManagedUikdi 2008/7/23 11:50 应用程序扩展 416 ×</li> <li>○ ManagedUikdi 416 ×<!--</td--><td>2008/7/23 11:50 金用程序扩展 12:49 2008/7/23 11:58 金用程序扩展 84:48 2008/7/23 11:58 金用程序扩展 84:48 2008/11/3 16:29 金用程序扩展 116:48 「病毒码版本 小网病毒码版本下载 病毒码版本导入到本地</td></li></ul>	2008/7/23 11:50 金用程序扩展 12:49 2008/7/23 11:58 金用程序扩展 84:48 2008/7/23 11:58 金用程序扩展 84:48 2008/11/3 16:29 金用程序扩展 116:48 「病毒码版本 小网病毒码版本下载 病毒码版本导入到本地
<ul> <li>● 本</li> <li>● 本</li></ul>	2010/08/17/1753 金用帽平 416.45 2008/77/23 11.58 应用程序扩展 84.48 2008/11/3 16.29 应用程序扩展 116.48 病毒码版本 外网病毒码版本下载 病毒码版本导入到本地
● UPDServiceClient.dl       2008/7/23 11.58       应用程序扩展       64 ×         ● MULL       2008/11/3 16.29       应用程序扩展       116 ×         ● MULL       2008/11/3 16.29       应用程序扩展       116 ×         ● MULL       ● MULL       2008/11/3 16.29       应用程序扩展       116 ×         ● MULL       ● MULL       ● MULL       116 ×       116 ×         ● MULL       ● MULL       ● MULL       116 ×       116 ×         ● MULL       ● MULL       ● MULL       116 ×       116 ×         ● MULL       ● MULL       ● MULL       116 ×       116 ×         ● MULL       ● MULL       ● MULL       116 ×       116 ×         ● MULL       ● MULL       ● MULL       116 ×       116 ×         ● MULL       ● MULL       ● MULL       ● MULL       116 ×         ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL         ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL         ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL       ● MULL	2008/7/23 11.58 ش馬爾厚宇區 84 48 2008/11/3 16.29 ش周围序于區 116 48 <b>「病毒码版本</b> 」 外网病毒码版本下载 病毒码版本导入到本地
※ XMtWrapper.dll      2008/11/9 16.29 前用程序扩展     16 ×            高线同步工具           家每码版本           小丁         「病毒码版本              外阿扑丁下载           补丁           病毒码版本           小阿病毒码版本下载           病毒码版本导入到本             砂信息列表:           正在下载补丁,请不要关闭程序!!           北丁           正在同步,这个步骤需要较长一段时间, 请耐心等待!	2008/11/3 16.29 前用照件算 116 K8 <b>病毒码版本</b> 小网病毒码版本下载 病毒码版本导入到本地
高线同步工具     「病毒码版本」       补丁     病毒码版本       外网补丁下载     补丁导入到本地       小网病毒码版本下载     病毒码版本导入到本.       砂塔信息列表:     正在下载补丁,请不要关闭程序!!       找到180条需要删除的热修复!     正在同步,这个步骤需要较长一段时间,请耐心等待!	□ □ × 病毒码版本 9
<b>高线同步工具 补丁 外</b> 四称丁下载 <b>补丁导入到本地 外</b> 四病毒码版本下载             「病毒码版本下载             「病毒码版本导入到本 <b>小</b> 野子 <b>小</b> 野子 <b>小</b> 丁 中美 <b>丁 「 「</b>	□ □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
斋线同步工具	□ □ × 病毒码版本 小网病毒码版本下载 病毒码版本导入到本地
高线同步工具       病毒码版本         补丁       病毒码版本         外网荪声可载       补丁导入到本地         小网病毒码版本下载       病毒码版本导入到本         司步信息列表:          正在下载补丁,请不要关闭程序!!          找到180条需要删除的热修复!          正在同步,这个步骤需要较长一段时间,请耐心等待!	
高线同步工具       「病毒码版本         补丁       「病毒码版本         小网补丁下载       补丁导入到本地         小网病毒码版本下载       「病毒码版本导入到本         同步信息列表:       正在下载补丁,请不要关闭程序!!         找到180条需要删除的热修复!       正在同步,这个步骤需要较长一段时间,请耐心等待!	□ □ • × 病毒码版本 小网病毒码版本下载 / 病毒码版本导入到本地 / , 请耐心等待!
高线向步上具 补丁 小阿补丁下载 补丁导入到本地 所毒码版本下载 病毒码版本导入到本 小阿病毒码版本下载 病毒码版本导入到本 小阿病毒码版本下载 病毒码版本导入到本 小阿病毒码版本下载 所毒码版本导入到本 小阿病毒码版本下载 所毒码版本导入到本 小田市事品。 二田市事品。 小田市事品。 二田市事 二田市事 二目 二田市市 二田市 二田市事 二田市 二田市 二田市 二田市 二田市 二田市 二田市 二田市	▲ 「病毒码版本 」 「病毒码版本下载」 病毒码版本导入到本地」 ④ 请耐心等待!
补丁 	▲ 病毒码版本 外网病毒码版本下载 病毒码版本导入到本地 病毒码版本导入到本地
小阿补丁下载 补丁导入到本地 外网病毒码版本下载 病毒码版本导入到本 即步信息列表: 正在下载补丁,请不要关闭程序!! 找到180条需要删除的热修复! 正在同步,这个步骤需要较长一段时间,请耐心等待!	9 // 外网病毒码版本下载 // 病毒码版本导入到本地
	9
司步信息列表: 正在下载补丁,请不要关闭程序!! 找到180条需要删除的热修复! 正在同步,这个步骤需要较长一段时间,请耐心等待!	1,请耐心等待!
正在下载补丁,请不要关闭程序!! 找到180条需要删除的热修复! 正在同步,这个步骤需要较长一段时间,请耐心等待!	9,请耐心等待!
正在下载补丁,请不要关闭程序!! 找到180条需要删除的热修复! 正在同步,这个步骤需要较长一段时间,请耐心等待!	》,请耐心等待!
找到180条需要删除的热修复! 正在同步,这个步骤需要较长一段时间,请耐心等待!	9,请耐心等待!
找到180条需要删除的热修复! 正在同步,这个步骤需要较长一段时间,请耐心等待!	3,请耐心等待!
正在同步,这个步骤需要较长一段时间,请耐心等待!	1,请耐心等待!
正在同步,这个步骤需要较长一段时间,请耐心等待!	同,请耐心等待!
IL LET 1977 AND EXTRACTARY AND THE PRODUCT AT 197	

当目录中没有 license 文件或 license 文件有问题时,将会显示加载 license 失败!

在同步过程中,我们可以看到在离线同步工具的目录下会自动生成 OfflineHotfix 目录, 在此目录下自动同步外网服务器上的补丁:



同步完成后,将离线同步工具目录拷贝到内网中心服务器任何目录下,并运行,点击"补 丁导入到本地":

▶ 离线同步工具 补丁 外网补丁下载 补丁导入到本地 外网病毒码版本下载 病毒码版本导入到本地
同步信息列表:
≫ 直线同步工具       补丁     病毒码版本       外网补丁下载     补丁导入到本地       历步信息列表:
正在复制文件,请等待! ● offlineDSrv X 发布成功 □ 确定

发布成功后,打开中心服务器安装目录的 download\AutoUpdate 目录,可以看到已经将补丁同步过来:

🔇 后退 🝷 🕥 🝷 🏂 🔎 搜索	📂 文件夹 🛛 🕼 🍞 🔀 🔛	•		
地址 @) 🫅 C:\Program Files\Venustech\Endpoint Security\ESServer\Download\AutoUpdate				
名称 ▲	大小 类型	修改日期 属性		
2004	文件夹	2010-8-7 11:47		
2005	文件夹	2010-8-7 11:47		
2006	文件夹	2010-8-7 11:47		
2007	文件夹	2010-8-7 11:47		
2008	文件夹	2010-8-7 11:47		
2009	<b>文件</b> 夹	2010-8-7 11:47		
2010	文件夹	2010-8-7 11:47		

然后打开服务器 web 管理界面,在在线补丁源页面中可以看到已经同步的补丁列表,

在补丁分发中可以将其分发到客户端:

6T#18	Ł				
a fair.	TA 2	al a			
	11.1		State Income to Interest of	11.7	1111
des treest		Actual All for Bill Planta Ref.	ADDAL DID AN ATTENTARY	12	
201010	18	AIT 把伸手机中的瞬间印刷力对这些东方的站	4年,且她是历十的美国历史也许这些办过此时	产業	
REAL	38	DET CLINE BASSOR BITELINGRAUSION	DAT CLIME MARGINARIZATION AND THE MARGINE	PX.	4
220044	315	SERL 编编算件 Louis 任性中的安全教师引起化冲出超热力代码	ERE 编集团件 Annual 任件中的安全基本可能比对自经和行利基	P#.	4
atta a	3.0	DESC WEIER Artist EPIPORE ##WTERPIOSES	THE WEAR AND DEPOSITE ADDRESS ADDRESS	78	4
10000	215	IN 新历十的新用印刷的内容把外门内间	DE ENTREMENTATION OF D	78	
1000	34	DE XPRIDARENTER DODD	IN MUSICAL PROPERTY IN LANCE	22	
Sec. 1	3%	Solution Texture TripS # 10588508(676805/058	BALLING CONTROL THE STREET CONCERNMENT	<b>F</b> #	
20120	10	GL FEBRERANNATER	GI TERRITERISTANISTICS	12	
mirann.	2.4	OF TEMPERATURE OF A DESCRIPTION OF A DES	CONTRACTOR OF CONT	7.8	

1958 創造庫	彩 要分为的	94FT	敗以分发任务  按补丁名提案			
E li	65.55	<u>86</u>	E.R.	S.I.	2222	紫布日
P.	重要	10013339	YINDOWS系统补丁	超球球病中的最同可能允许执行代码	\$204-043	
17	重要	10005035	VIRIONS系统补丁	Windows 内核和 LIASS 中的講問可能允许特权提升	MSD4-044	
P	重要	100000000	VIEDOVS系统补丁	Windows 中的最同时能导致信息测载	MS06-001	
F	₩ <b>X</b>	12885834	VINDOVS系统补丁	许可证记录服务中的编词可能允许执行代码	\$\$05-010	
9	₽ <b>R</b>	10081701	YINDOWS系统补丁	INTNL 编辑信件 ActiveS 经件中的安全课得可能允许执行代码	\$505-013	
P	声素	10867282	软件系统补工	Internet Explorer 的展积性安全更新	NS05-014	
P.	声重	10888113	YINDOVS系统补丁	超這時提对象庫中的偏視可能允许這程执行代码	MS05-015	
P	-	120122544	vintors系统补丁	清意以列展多中的局限可能允许执行代码	MS06-017	
P	重要	<u>XR090959</u>	VIEDOVS系统补丁	Windows 内核的晶洞可能允许特权提升和拒绝服务	MS06-018	
-	声音	1000000	教神系統計工	Internet Funlarer 的思想性安全更新	#\$25-020	

离线同步工具导入外网病毒码

将 license 放在离线同步工具目录下,并拷贝到可上互联网的机器上,点击运行

offlineDSrv,并点击"外网病毒码版本下载":

补丁	,,有毒码版本	
外网补丁下载	补丁导入到本地外网病毒码版本下载	病毒码版本导入到本地
同步信息列表:		
正在同步病毒码版	本,请不要关闭程序!!	
正在处理防病毒软	"件信息 <b>!</b>	
正在处理防病毒软 Symantec防病毒防 趋势防病毒防病毒	:件信息! :病毒没有更新,忽略! :没有更新,忽略!	
正在处理防病毒软 Symantec防病毒防 趋势防病毒防病毒 瑞星防病毒防病毒 McAfee防病毒防病	:件信息! :病毒没有更新,忽略! :没有更新,忽略! :没有更新,忽略! :毒没有更新,忽略!	
正在处理防病毒软 Symantec防病毒防 趋势防病毒防病毒 瑞星防病毒防病毒 端CAfee防病毒毒防病。 物还逐舰防病毒防病。 物还还原金素防病。	:件信息! :病毒没有更新,忽略! 没有更新,忽略! :毒没有更新,忽略! :毒没有更新,忽略! :>没有更新,忽略! :>:	
正在处理防病毒软 Symantec防病毒防病毒防 趋势防病毒防病毒防病毒防病毒 McAfee防病毒防病毒 微软防病毒防病 360杀毒防病毒 360杀毒下病毒 公在五百五五 公开	:件信息!  病毒没有更新,忽略!  没有更新,忽略!  毒没有更新,忽略!  毒没有更新,忽略!     注,忽略!       二::::::::::::::::::::::::::::::::	
正在处理防病毒软 Symantec防病毒防 趋势防病毒防病毒防 瑞星防病毒防病病毒防病病 MCAfee防病病毒防病病 躯诊舰防病毒防病病 360杀毒防病毒防病毒 360杀毒防病毒没 有	:件信息! :病毒没有更新,忽略! 没有更新,忽略! :海没有更新,忽略! :海没有更新,忽略! :没有更新,忽略! :没有更新,忽略! :理完成!	
正在处理防病毒软 Symantec防病毒防 趋势防病毒防病毒防 瑞星防病毒防病毒 端星防病毒防病毒 不不是的病毒防病毒 不不是一个。 一个。 一个。 一个。 一个。 一个。 一个。 一个。 一个。 一个。	:件信息! :病毒没有更新,忽略! 没有更新,忽略! :毒没有更新,忽略! :>没有更新,忽略! :没有更新,忽略! :没有更新,忽略! :理完成!	
正在处理防病毒软 Symantec防病毒防 趋势防病毒防病毒防 瑞星防病毒防病毒 水石fee防病毒防病病 都区逐舰防病毒防病病 额欲逐度的病毒防病病 360杀毒防病毒 360杀毒的病毒 360杀毒的病毒 分	:件信息! :病毒没有更新,忽略! 没有更新,忽略! :海没有更新,忽略! :海没有更新,忽略! :没有更新,忽略! :理完成!	

同步完成后,将离线同步工具目录拷贝到内网中心服务器任何目录下,并运行,点击"补 病毒码版本导入到本地":

禺线回步上具	
补丁	病毒码版本
外网补丁下载 补丁导入到本地	外网病毒码版本下载 病毒码版本导入到本地
]步信息列表:	
で左阜 \ 疾事职版术 诗不重关闭程度♥ ♥	
兩毒码检测方法处理完成!	

发布成功后,打开 web8833 页面上的安全基线—》防病毒软件策略,然选一个防病毒软件,进入该策略的编辑页面,点击"选择病毒码版本"

防病毒软件策略		
除合书特世体世		
防病母软件官埋		
策略名称	防病毒软件管理在线	
策略描述		
防病毒软件类型	360杀毒	
防病毒软件进程	同一进程可以指定多个MD5码,用分号隔开 进程名称 005码	编辑 删除
		样本计算 添加
	360Tray. exe	🥒 🗙
进程延迟检测时间	1 分钟	
是否检查病毒码版本	◎否○是	
要求的病毒码版本	选择病毒码版本	
病毒码延迟更新的最长天 数	(0为不限制)只有当病毒码版本	满足的时候才起作用
病毒码升级网址		
生效时间	⊙所有时间 ○工作时间 ○非工作时间 ○以下时间段	
	开始时间         结束时间         第           2012-03-10         9:00         2012-03-10         13:30	算错 别除 逐加
在线模式	🗹 在线时生效 🗌 离线时生效	
策略应用对象	<u>查看及编辑</u>	

此时会弹出一个提窗口,如果在外网服务器上该防病毒软件有新增的病毒码版本,同步

完成后该窗口就会出现相应的新的病毒码:

<b>访病毒软件类型:</b> Symante	≥c防病毒		
防病毒软件版本	病毒码版本	发布时间	选择
Symantec防病毒	20050517	2009-06-18	选择
9.0	20090516	2009-07-08	选择
10	20050518	2009-09-17	选择
11.0	20100801	2010-08-02	选择

离线同步工具相关异常页面:

(1) 当运行离线补丁工具的计算机没有安装 framework 时,提示如下:

离线	同步工具	
<b>补丁</b> - 外网	网补丁下载 补丁导入到本地 外网病毒码版本下载 病毒码版	医人到本地
步信息	息列表:	
正在下	TODO: <file description=""></file>	
	TODO: 《File description〉遇到问题需要关闭。我们对此引起的不便表示抱歉。	<b>&gt;&gt;</b>
	如果您正处于进程当中,信息有可能丢失。 请将此问题报告给 Microsoft。 我们已经创建了一个错误报告,您可以将它发送给我们。我们将 此报告视为保密的和匿名的。	
	要查看这个错误报告包含的数据, <u>请单击此处。</u> 发送错误报告 (2) <u>不发送</u> (	<u>D)  </u>

(2) 当离线补丁工具目录中没有放入 license 授权,运行该工具,提示如下:

≫ 离线同步工具	
补丁	病毒码版本导入到本地
同步信息列表:	
正在下载补丁,请不要关闭程序!!	*
加载license失败!	

(3) 当离线补丁工具运行的计算机没有同外网连接时,提示如下:

≫ 离线同步工具	
补丁 外网补丁下载 补丁导入到本地 外网病毒码版本下载 3	<b>病毒码版本导入到本地</b>
同步信息列表:	
正在下载补丁,请不要关闭程序!!	A
关联到WebService失败!	

(4) 在下载外网补丁的过程中,网络中断,提示如下:



(5) 补丁导入本地时,如果导入的计算机没有安装中心服务器时,提示如下:

≫ 离线同步工具		- C <b>X</b>
补丁 外网补丁下载 补丁导入到本地	「病毒码版本」 外网病毒码版本下载	病毒码版本导入到本地
同步信息列表:		
找不到天珣中心服务器,无法导入补丁!		*

### Radius By Pass 工具

RadiusBypass 适用与网络准入跟 AD 域结合使用的网络准入认证方案.当 AD 域出现 故障时,开启 RadiusBypass 工具,可及时将准入认证方案切换成只认证客户端,终端网络准入 认证不需要输入 AD 域的用户名密码,就可以通过网络准入认证。

该工具需要运行在安装有 Radius 服务器的机器上。

💑 网络碓入Bypass控制工具	E	×
Radius服务状态:	运行中	
网络准入Bypass状态:	禁用	
注意: 必须启动Radius	服务后网络准入Bypass功能才生效。	
切换到Bypass状;	态退出	

### Radius 故障告警工具

工具适用于用户名密码登录的网络准入认证方式的告警.将告警日志存放到 FTP 服务器

上.

工具需配置 RADIUS,域的参数,及 FTP 服务器的地址.

用户名:填写域中的用户名,

密码:用户的密码。

目录名:名称与天珣配置页-基本配置-用户组-目录服务中的目录服务名称对应,不是域的 名字。

▶ 首页 白…●基本配置	使用单位:厦门银行 <u>目录服务</u> 用戶	〕 <sup>2</sup> 組	
<ul> <li>□ 按需支援操作员</li> <li>□ ● 策略服务器</li> <li>□ ○ 管理网段</li> </ul>	目录服务		
<b>OIP</b> 组 <b>O</b> 部门	目录名称	testwork	*
◎终端注册	目录服务类型	Active Directory Server	-
·····································	目录服务路径	dc=venus, dc=com	*

Radius IP 地址:可以填写多个,每个 ip 以,隔开

HELL MAZES	advestort	_
нга:	lauserest	
密码:	*****	
目录名:	testwork	_
radius IP地	172. 18. 20. 23	_
	*多个服务器以 , 隔开	
日志上报配置		
日志上报配置 ftp地址:	172. 18. 20. 3	
日志上报配置 ftp地址: ftp端口:	172. 18. 20. 3 21	
日志上报配置 ftp地址: ftp端口:	172. 18. 20. 3 21	
日志上报配置 ftp地址: ftp端口: ftp用户名:	172. 18. 20. 3 21 user	
日志上报配置 ftp地址: ftp端口: ftp用户名: ftp用户密码:	172. 18. 20. 3 21 user 123456	
日志上报配置 ftp地址: ftp端口: ftp用户名: ftp用户密码:	172. 18. 20. 3 21 user 123456	
日志上报配置 ftp地址: ftp端口: ftp用户名: ftp用户密码:	172. 18. 20. 3 21 user 123456	