新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/8/4- 2008/8/17 第73期

负载均衡器 / MH系列报导

技术浅谈与应用 - 监控记录种类说明及如何妥善保存监控记录

身为一个管理人员，除了必须控制管理公司内部所有大大小小的信息系统、设备之外，信息记录的妥善保存也是相当重要的项目之一，新软系统MH系列产品中【监控记录】记录着的各项使用者透过产品的一切操作行为信息。这些信息分为**流量监控**、**事件监控**、**连机记录**、**应用程序管制记录**、**内容管制记录**等五大类。在这些监控记录里，管理者该如何才能妥善的保存所有的记录，以做为日后公司存查的依据？这是管理人员必去须了解的。

流量监控：

可在设定【管制条例】时，于条例内进行设定；或在【系统管理】处勾选。而两种设定方式的差异之处分别为，在【管制条例】中的设定时，只有设定的该项【管制条例】会详细记录数据封包联机。而在【系统管理】中设定时，会让目的与来源为MH产品的封包皆做详细记录。系统管理员可在流量监控记录里，查询目前进出MH产品各个联机状态，包括：联机起始时间、来源地址、目的地址与处置方式等。

事件监控：

记录产品系统组态参数值(System Configurations)更改的内容，包含更改者、更改时间、更改的参数及登入的IP地址…等。系统管理员可经由此事件监控功能，了解事件发生的时间详细说明。

连机记录：

记录MH产品中所有的联机信息。若联机发生问题时，系统管理员可凭借着此信息，进一步的了解问题的所在，以及对目前联机状态作记录。

应用程序管制记录：

记录被MH产品阻挡的应用程序存取信息，系统管理员可利用此功能，立即得知应用程序的阻挡情形。

内容管制记录：

记录被MH产品所阻挡的网站存取、网页Script执行、文件下载、文件上传信息，系统管理员可利用此功能，立即得知阻挡情形。

而关于记录的备份方面，系统管理者除了可使用手动方式，随时于系统各个监控记录接口上点选「下载记录」外，也可利用系统内建的监控备份功能『电子邮件监控记录』来设定系统当记录文件达到特定容量时，自动发出 E-mail 提醒管理员流量监控与事件监控的记录，或利用『远程记录』功能让指定的 Syslog Server 实时接收 MH 产品的监控记录备份，完成妥善保存以方便日后公司存查使用。

电子邮件监控记录：

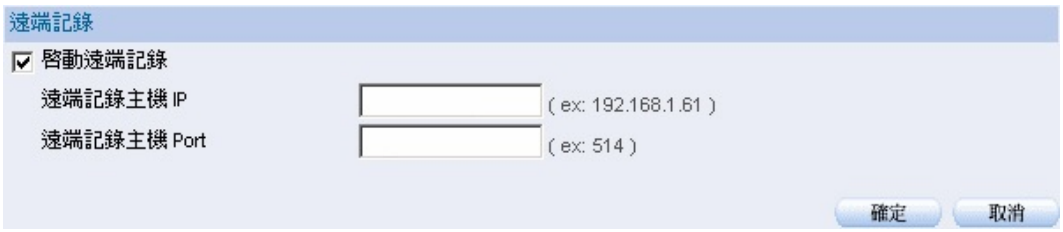
于【系统管理】→【系统设定】中，勾选【开启电子邮件警讯通知】功能，并设定相关数据即可，完成设定后，每当监控记录文件到达 300 Kbytes 时，系统就会将到目前为止所累积的监控记录，邮寄监控记录给设定中所指定的收件者。

电子邮件监控记录设定画面

设定完成画面

远程记录：

启用远程记录功能后，可将监控记录传送到所指定的 Syslog Server 做备份的动作。



远程记录设定画面

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 3A Server 的好；让管理者感受的到

新软系统在 MH 系列产品中使用了 3A 的功能来协助管理者能够更轻松且完善、详细的管理公司内部各种信息系统及讯息。而 3A 则分别是 Authentication、Authorization、Accounting 的简称，简单明确的让公司内部所有使用者在经过 MH 产品做联机时，都必须经过 MH 的『认证』身份后，再经由『管制』给于授权此身份所能使用的联机权限，并且再将使用者所有的联机信息详细的『统计及记录』做成监控报告，以供管理人员分析及调整各项网络政策之设定。

Authentication：产品内建认证系统，并支持外部远程验证拨入使用者服务(RADIUS)及 POP3 认证，多样化的验证设计，支持了多样化的使用环境，管理人员可简单的因应各种使用环境的需求。

Authorization：管理人员可利用 Policy 管制功能，搭配各项管制条例，可严格控管所有进出的联机，让不同部门、不同群组、不同身份的使用者享有不同的权限，新软系统设计的管制条例明确易懂，让管理人员容易上手也易于控制。

Accounting：MH 系统产品提供了巨细靡遗的联机统计报告，管理人员可依据报告内容做分析，方更将网络政策做最适当的调整，以及利用报告功能也可做最实时的线路监控。

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
Jul 30 09:44:40	192[illegible]	[illegible].168.[illegible]	TCP	1863 => 80	34 KB	✓
Jul 30 09:44:40	192[illegible]	[illegible].168.[illegible]	TCP	1864 => 80	23 KB	✓
Jul 30 09:44:40	192[illegible]	[illegible].168.[illegible]	TCP	1865 => 80	29 KB	✓
Jul 30 09:44:40	192[illegible]	[illegible].168.[illegible]	TCP	1866 => 80	26 KB	✓
Jul 30 09:44:40	192[illegible]	[illegible].168.[illegible]	TCP	1867 => 80	7 KB	✓
Jul 30 09:44:33	192[illegible]	192[illegible]	UDP	68 => 67 (WAN1)	328 B	✓

時間	管理員名稱	IP 位址	事件	內容
Jul 29 12:25:43	admin	[illegible]247	[Policy Object] Remove [IPSec Autokey] (Name : test2)	
Jul 29 12:25:41	admin	[illegible]247	[Policy Object] Remove [IPSec Autokey] (Name : test1)	
Jul 29 12:25:37	admin	[illegible]247	[Policy Object] Remove [Trunk] (Name : tt1)	
Jul 29 12:25:34	admin	[illegible]247	[Policy Object] Remove [Trunk] (Name : tt2)	
Jul 29 12:25:32	admin	[illegible]247	[Policy Object] Pause [Trunk] (Name : tt2)	

時間	事件
Jul 29 12:44:20	pluto[1256]: packet from 220[illegible]: initial Main Mode message received on 59.[illegible]0 but no connection has been authorized
Jul 29 12:44:20	pluto[1256]: packet from 220[illegible]: received Vendor ID payload [Dead Peer Detection]
Jul 29 12:44:20	pluto[1256]: packet from 220[illegible]: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
Jul 29 12:44:20	pluto[1256]: packet from 220[illegible]: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
Jul 29 12:44:20	pluto[1256]: packet from 220[illegible]: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
Jul 29 12:44:20	pluto[1256]: packet from 61.[illegible]: initial Main Mode message received on 59.[illegible]0 but no connection has been authorized

流量、事件、联机监控报告画面截图

除此之外还有其它多项监控报告功能，可供管理人员做更详细的信息控管。

在如此层层把关的环境下，不但能让公司更有制度的运作，管理人员也只需利用 MH 的 UI 接口即可轻松管理所有大大小小事情，不需要像从前般的控制多台机器而手忙脚乱，当然 MH 产品的功能决不只有如此，同时还拥有 SPI 防火墙、线路实时备援、负载均衡、带宽分流、合并带宽的功能，也提供了完整的 VPN 解决方案（SSL VPN、IPSec / PPTP VPN、VPN Trunk），并同时具备了 IM / P2P 管制、中毒警示功能…等多项功能，一机满足多项需求，新软系统 MH 系列产品绝对是各公司最佳的管理产品选择。

如需了解更详细的产品信息，欢迎至 http://www.nusoft.com.tw/

文 陈殿鸿 kim@nusoft.com.tw