第5章 日志存储与分析

日志数据主要是根据数据的存储格式、日志数据所需存储空间、日志数据检索速度、存储所需成本等需求策略进行存储。本节首先介绍日志数据的存储格式，主要有基于文本的日志文件存储、二进制文件存储以及压缩文件的存储。随后，综合存储日志所需的空间的大小和检索速度，介绍本地数据库存储和以 Hadoop 存储为代表的分布式存储策略。

5.1 日志审计与分析系统实时监视实验

【实验目的】

日志审计与分析系统提供实时监视功能，可以监视最近时间内发生的事件，包括外部事件、告警事件等。本实验通过向日志审计与分析系统发送防火墙日志来查看实时监视结果。

【知识点】

实时监视、外部事件。

【实验场景】

近期，A 公司安全运维工程师小王发现公司防火墙的 IP 访问频繁，为了实时了解防火墙日志的具体信息，及时发现并处理安全隐患，小王需要对防火墙进行实时监控。请思考应如何操作。

【实验原理】

在虚拟机中使用 UDPsender 向日志审计与分析系统服务器发送防火墙日志，用户单击“事件”→“实时监视”→“接受的外部事件”，可以查看接收的防火墙日志，在停止接收日志后在“实时监视”中查看相关告警事件。

【实验设备】

- 安全设备：日志审计与分析设备 1 台。
- 主机终端：Windows XP 主机 1 台。

【实验拓扑】

日志审计与分析系统实时监视实验拓扑图如图 5-1 所示。

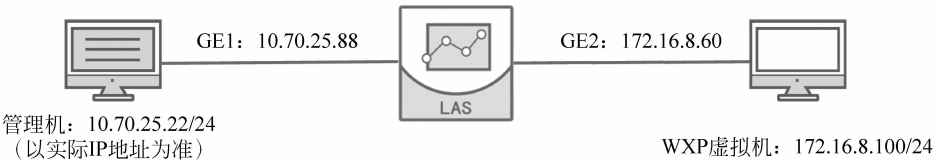

图 5-1　日志审计与分析系统实时监视实验拓扑图

【实验思路】

（1）登录 WXP 虚拟机向日志服务器发送防火墙日志。

（2）以管理员 admin 用户的身份登录日志审计与分析系统。

（3）查看“实时监视”内容。

（4）双击查看日志信息。

【实验步骤】

（1）在管理机端单击 Xshell 图标，打开 Xshell。

（2）在会话框中单击“新建”按钮，创建新的会话。

（3）在“主机”栏中输入日志审计与分析系统 GE1 接口的 IP 地址“10.70.25.88”（以实际 IP 地址为准），其他设置保持不变，单击“确定”按钮。

（4）新建的会话会在“所有会话”中显示，选中“新建会话”，单击“连接”按钮。

（5）单击“一次性接受”按钮。

（6）在“请输入登录的用户名”一栏中输入用户名 admin，单击“确定”按钮。

（7）在“密码”栏中输入密码“@1fw＃2soc＄3vpn”，单击“确定”按钮。

（8）成功登录日志审计与分析系统后台。

（9）输入命令“secfox -e eth1 -p 172.16.8.60 -m 255.255.255.0”，设置日志审计与分析系统 GE2 接口的 IP 地址。其中，“172.16.8.60”是 GE2 口的 IP 地址，“255.255.255.0”是 GE2 口的子网掩码。按 Enter 键，出现“modify ip ...”，说明接口信息配置成功。

（10）打开浏览器，在地址栏中输入日志审计与分析系统的 IP 地址“https://10.70.25.88(以实际 IP 地址为准)”，单击“继续浏览此网站”按钮，打开平台登录界面。

（11）输入管理员用户名/密码“admin/!1fw@2soc＃3vpn”，单击“登录”按钮，登录日志审计与分析系统。

（12）系统设置的密码有效期为 7 天，当登录系统后收到更改密码提示时，单击“确定”按钮，更改系统密码。

（13）在“原始密码”一栏输入原始密码“!1fw@2soc＃3vpn”。在“新密码”一栏输入“!1fw@2soc＃3vpn”，与原始密码相同。在“确认新密码”一栏输入“!1fw@2soc＃3vpn”，单击“确定”按钮。

（14）单击浏览器中的“工具”→“兼容性视图设置”。

（15）输入日志审计与分析系统的 IP 地址“https://10.70.25.88”（以实际 IP 地址为准），单击“添加”按钮，添加网站兼容性视图。

（16）单击“关闭”按钮，退出设置。

（17）进入日志审计与分析系统后，单击“系统”→“系统维护”，可看到系统“IP 地址配置 1”为“172.16.8.60”。

（18）将管理机时间与日志审计与分析系统时间统一。在日志审计与分析系统中，单击“系统”→“系统维护”，接着单击“时间校对设置”框中的“手动校时”选项。

（19）单击“时间”一栏的钟表图案。

（20）选择与管理机统一的时间。

（21）单击屏幕空白处，退出设置。

（22）单击“修改时间”，完成日志审计与分析系统时间的手动修改。

（23）修改成功后，系统会跳转至登录界面，重新输入用户名/密码“admin/!1fw@2soc#3vpn”，登录日志审计与分析系统。

（24）重新登录后，查看系统界面右下方的时间，与管理机时间相同。

（25）登录实验平台，打开虚拟机 WXPSP3，对应实验拓扑中的右侧设备，如图 5-2 所示。

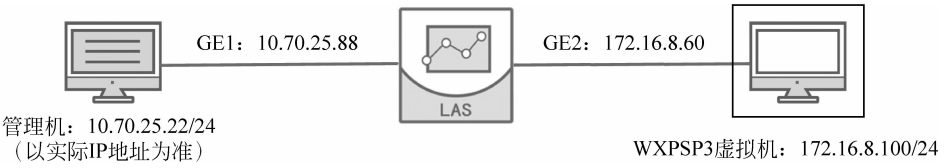

图 5-2　打开虚拟机 WXPSP3

（26）进入虚拟机后，为保证日志审计与分析系统收到的日志文件时间与虚拟机时间一致，首先查看虚拟机的系统时间与管理机的系统时间是否一致，如果不一致，则双击虚拟机界面右下角的时间进行调整。

（27）根据管理机时间对虚拟机时间进行调整，时间确定后单击“确定”按钮。

（28）进入虚拟机桌面，打开桌面上的“实验工具”。

（29）单击文件夹 UDPSender。

（30）UDPsender 是模拟防火墙日志发送的工具，双击图标“UDPsender.exe”，打开文件夹中的日志发送工具。

（31）配置日志发送的相关信息，“协议”设置为 Syslog，“方式”设置为“按速度发送”，“速度”输入 5，然后单击“初始化通信”。

（32）“消息来源”设置为“从文件”，单击“...”按钮，选择目标日志文件。

（33）从查找范围中的“桌面”进入“实验工具”目录，单击 UDPSender 文件夹。

（34）进入 logfiles 进行日志文件选择，本实验选择“FW_LOG_DEOM.log”，再单击“打开”按钮。

（35）在目标端设置中，选中序号为 0 的目标，单击“编辑”。

(36) 将“目的 IP 地址”设置为“日志服务器的 IP 地址”,本实验设置为“172.16.8.60”,端口设为 514。

(37) 完成设置后,核对信息配置是否正确,然后单击“发送”按钮。

(38) 完成日志发送过程后,按照步骤(1),在管理机中登录日志审计与分析系统平台,依次单击“资产”→“资产日志”,如图 5-3 所示。

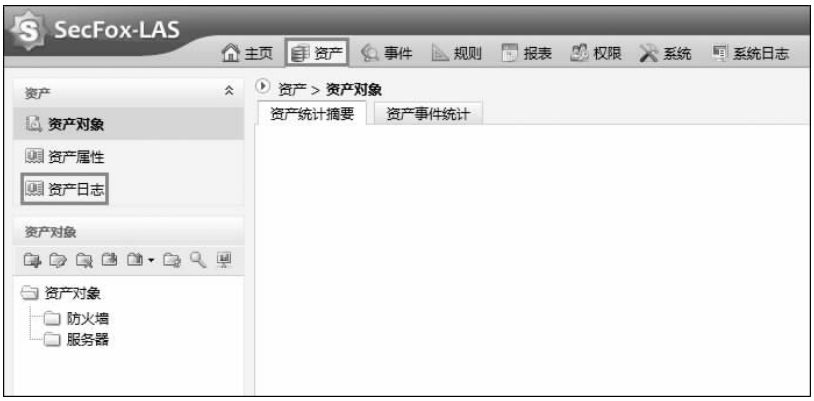

图 5-3　进入资产日志界面

(39) 选中资产地址“172.16.8.100”,单击“允许接收”和“启用”按钮,以允许日志审计与分析系统接收日志,并启用“是否告警”,如图 5-4 所示。

图 5-4　管理资产日志

(40) 修改“配置告警间隔”,系统默认告警间隔为 1 天,在本实验中将其设置为 1 分钟,以便于观察实验结果,如图 5-5 所示。

图 5-5　配置告警间隔

【实验预期】

(1) 在日志审计与分析系统中可以查看到接收的日志文件。

(2) 停止日志发送后在实时监视中可以查看告警信息。

【实验结果】

（1）在管理机中重新登录日志审计与分析系统平台，依次单击“事件”→“实时监视”→“接收的外部事件”，如图 5-6 所示。

图 5-6　接收的外部事件

（2）可以在“接收的外部事件”中实时查看发送过来的日志信息，如图 5-7 所示。

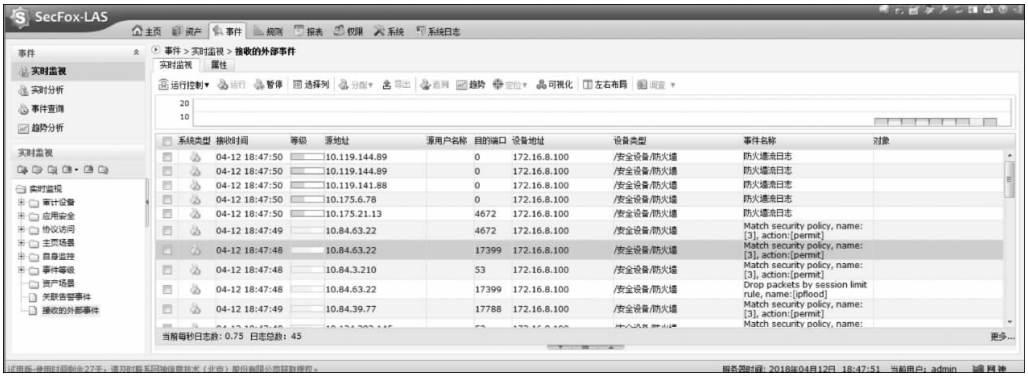

图 5-7　接收日志成功

（3）登录实验平台对应实验拓扑右侧的 WXP 虚拟机，如图 5-8 所示。

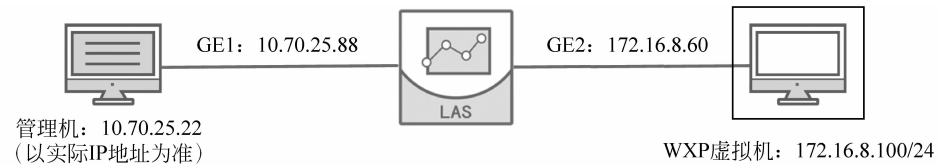

图 5-8　进入虚拟机 WXP

（4）停止发送日志，在 UDPsender 界面单击“停止”按钮。

（5）在管理机中登录日志审计与分析系统平台，依次单击“事件”→“实时监视”→“主页场景”→“最近 5 分钟产生的告警事件”，进入“属性”界面调整时间设置，将“最近发生时间”设置为 5 天，如图 5-9 所示。

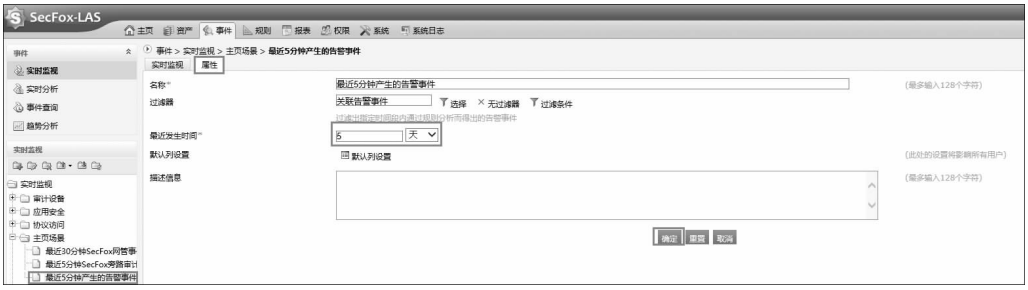

图 5-9　时间设置

（6）在“最近 5 分钟产生的告警事件”的实时监视界面，可以看到产生的告警事件，如图 5-10 所示。

图 5-10　实时监视告警事件

（7）同样在“实时监视”模块，依次单击“事件等级”→“警告事件”，进入“属性”界面调整时间设置，将“最近发生时间”设置为 5 天，如图 5-11 所示。

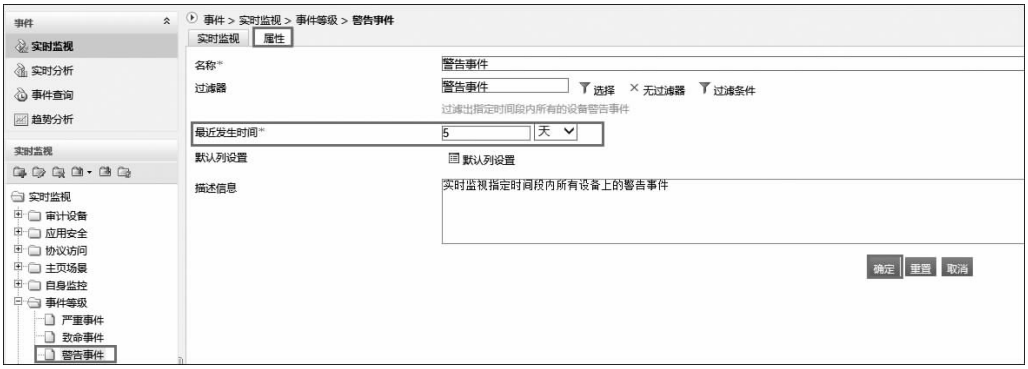

图 5-11　日志文件基本信息

（8）在“警告事件”的实时监视界面，可以看到产生的告警事件，如图 5-12 所示。

图 5-12　产生的告警事件

(9) 综上所述,日志审计与分析系统可以对设备进行日志采集,并可以监测告警事件,更好地完成对设备的实时监视。

【实验思考】

(1) 日志发送工具中的 514 端口是否可以修改,为什么?

(2) 实时监视除了及时发现告警,还有什么其他功能?

5.2 日志审计与分析系统实时分析实验

【实验目的】

日志审计与分析系统提供实时分析功能,可以分析最近时间内发生的事件,包括外部事件、告警事件等。本实验通过向日志审计与分析系统发送防火墙日志,构造实时分析场景,查看实时分析结果。

【知识点】

实时分析、日志统计。

【实验场景】

A 公司的日志审计与分析设备由安全运维工程师小王负责。小王希望通过日志审计与分析系统对收集到的防火墙日志进行实时分析,及时发现运维过程中的问题,并及时处理。请思考应如何实现。

【实验原理】

日志审计与分析系统提供实时分析功能,可以对接收的信息以柱图或饼图等图形向管理员提供实时分析信息。在虚拟机中使用 UDPsender 向日志审计与分析系统服务器发送防火墙日志,用户单击“事件”→“实时分析”,可以查看防火墙日志的实时分析图表。

【实验设备】

- 安全设备：日志审计与分析设备 1 台。
- 主机终端：Windows XP 主机 1 台。

【实验拓扑】

日志审计与分析系统实时分析实验拓扑图如图 5-13 所示。

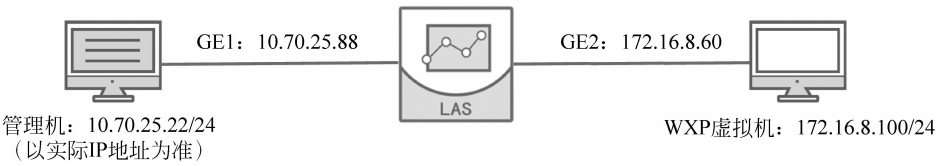

图 5-13　日志审计与分析系统实时分析实验拓扑图

【实验思路】

(1) 配置日志平台网络接口。

(2) 登录 WXP 虚拟机向日志服务器发送防火墙日志。

(3) 以管理员 admin 用户的身份登录日志审计与分析系统。

(4) 查看事件的实时分析图表。

【实验步骤】

(1) 在管理机端单击 Xshell 图标，打开 Xshell。

(2) 在会话框中单击“新建”按钮，创建新的会话。

(3) 在“主机”栏中输入日志审计与分析系统 GE1 接口的 IP 地址“10.70.25.88”(以实际 IP 地址为准)，其他设置保持不变，单击“确定”按钮。

(4) 新建的会话会在“所有会话”中显示，选中“新建会话”，单击“连接”按钮。

(5) 单击“一次性接受”。

(6) 在“请输入登录的用户名”一栏中输入用户名 admin，单击“确定”按钮。

(7) 在“密码”栏中输入密码“@1fw#2soc$3vpn”，单击“确定”按钮。

(8) 成功登录日志审计与分析系统后台。

(9) 输入命令“secfox -e eth1 -p 172.16.8.60 -m 255.255.255.0”，设置日志审计与分析系统 GE2 接口的 IP 地址。其中，“172.16.8.60”是 GE2 口的 IP 地址，“255.255.255.0”是 GE2 口的子网掩码。按 Enter 键，出现“modify ip ...”，说明接口信息配置成功。

(10) 打开浏览器，在地址栏中输入日志审计与分析系统的 IP 地址“https://10.70.25.88(以实际 IP 地址为准)”，单击“继续浏览此网站”按钮，打开平台登录界面。

(11) 输入管理员用户名/密码“admin/!1fw@2soc#3vpn”，单击“登录”按钮，登录日志审计与分析系统。

(12) 系统设置的密码有效期为 7 天，当登录系统后收到更改密码提示时，单击“确

定”按钮，更改系统密码。

（13）在“原始密码”一栏输入原始密码“!1fw@2soc#3vpn”。在“新密码”一栏输入“!1fw@2soc#3vpn”，与原始密码相同。在“确认新密码”一栏输入“!1fw@2soc#3vpn”，单击“确定”按钮。

（14）单击浏览器中的“工具”→“兼容性视图设置”。

（15）输入日志审计与分析系统的IP地址“https://10.70.25.88”，单击“添加”按钮，添加网站兼容性视图。

（16）单击“关闭”按钮，退出设置。

（17）进入日志审计与分析系统后，单击“系统”→“系统维护”，查看到系统“IP地址配置1”为“172.16.8.60”。

（18）将管理机时间和日志审计与分析系统时间统一。在日志审计与分析系统中，单击“系统”→“系统维护”，接着单击“时间校对设置”框中的“手动校时”选项。

（19）单击“时间”一栏的钟表图案。

（20）选择与管理机统一的时间。

（21）单击屏幕空白处，退出设置。

（22）单击“修改时间”，完成日志审计与分析系统时间的手动修改。

（23）修改成功后，系统会跳转至登录界面，重新输入用户名/密码“admin/!1fw@2soc#3vpn”，登录日志审计与分析系统。

（24）重新登录后，查看系统界面右下方的时间，与管理机时间相同。

（25）登录实验平台，打开虚拟机WXP，对应实验拓扑中的右侧设备，如图5-14所示。

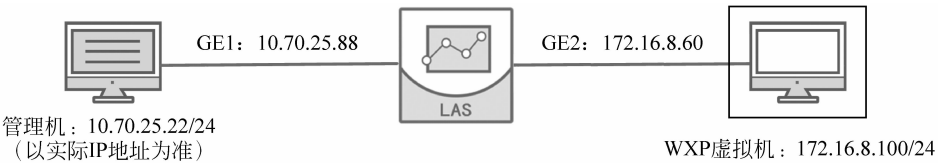

图5-14　打开虚拟机WXP

（26）进入虚拟机后，为保证日志审计与分析系统收到的日志文件时间与虚拟机时间一致，首先查看虚拟机的系统时间与管理机的系统时间是否一致，如果不一致，则双击虚拟机界面右下角的时间进行调整。

（27）根据管理机时间对虚拟机时间进行调整，时间确定后单击“确定”按钮。

（28）进入虚拟机桌面，打开桌面上的“实验工具”。

（29）单击文件夹UDPSender。

（30）UDPsender是模拟防火墙日志发送的工具，双击图标“UDPsender.exe”，打开文件夹中的日志发送工具。

（31）配置日志发送的相关信息，“协议”设置为Syslog，“方式”设置为“按速度发送”，“速度”输入5，然后单击“初始化通信”。

（32）“消息来源”设置为“从文件”，单击“...”按钮，选择目标日志文件。

(33) 在查找范围中的“桌面”上进入“实验工具”目录，单击 UDPSender 文件夹。

(34) 进入 logfiles 进行日志文件选择，本实验选择“FW_LOG_DEOM.log”，再单击“打开”按钮。

(35) 在目标端设置中，选中序号为 0 的目标，单击“编辑”按钮。

(36) 将“目的 IP 地址”设置为“日志服务器的 IP 地址”，本实验设置为“172.16.8.60”，端口设置为 514。

(37) 完成设置后，核对信息配置是否正确，然后单击“发送”按钮。

(38) 完成日志发送过程后，按照步骤(1)，在管理机中登录日志审计与分析系统平台，依次单击“资产”→“资产日志”，如图 5-15 所示。

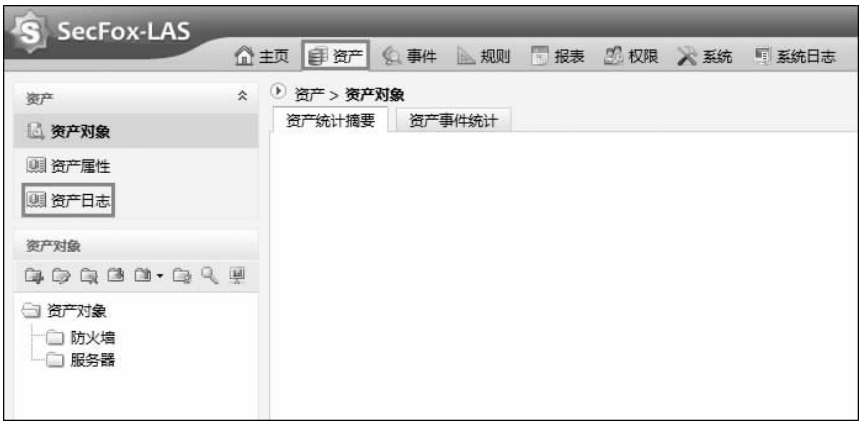

图 5-15　进入资产日志界面

(39) 选中资产地址“172.16.8.100”，单击“允许接收”和“启用”按钮，以允许日志审计与分析系统接收日志，并启用“是否告警”，如图 5-16 所示。

图 5-16　管理资产日志

【实验预期】

(1) 对事件的数量进行实时分析。

(2) 对告警事件的产生进行实时分析。

【实验结果】

(1) 在管理机中重新登录日志审计与分析系统平台，依次单击“事件”→“实时分析”→“主页场景”→“各事件总数统计”，如图 5-17 所示。