

# 面向多平台的日志远程采集系统研究

杨锋英<sup>1</sup>, 刘会超<sup>1,2</sup>

(1. 黄淮学院 信息工程学院, 河南 驻马店 463000;  
2. 武汉大学 计算机学院, 湖北 武汉 430072)

**摘要:** 日志对于系统的日常运维、审计及入侵检测等具有重要作用, 对日志进行远程集中化管理是日志管理的有效手段。由于不同操作系统平台上支持的日志格式不统一, 传统上很难将大型网络中不同系统的日志远程采集到集中的日志服务器上。nxlog 是一种支持多平台的功能强大的日志采集工具, 部署方便, 可以在目标系统上持续稳定地收集系统日志, 并支持以多种日志格式和传输模式将日志发送到远程日志服务器。同时, Syslog 作为一种工业协议, 也得到了越来越多的支持。基于 nxlog 并配合成熟的日志服务器可以构建灵活可靠的系统日志远程采集系统。实际运行结果表明该方案可有效解决大型网络中系统日志远程采集的问题。

**关键词:** 网络安全; 系统日志; 日志采集; nxlog; Syslog; 多平台

**中图分类号:** TP309

**文献标识码:** A

**文章编号:** 1673-629X(2014)07-0149-04

doi: 10.3969/j.issn.1673-629X.2014.07.037

## Research on Remote Log Collection System for Multi-platform

YANG Feng-ying<sup>1</sup>, LIU Hui-chao<sup>1,2</sup>

(1. School of Information Engineering, Huanghuai University, Zhumadian 463000, China;  
2. School of Computer, Wuhan University, Wuhan 430072, China)

**Abstract:** Log plays an important role in the system daily operation, audit and intrusion detection, and the mode of the remote centralized management is an effective means for log management. Because of the different log formats for different operation system, traditionally, it is difficult to gather the log of each system, and transmit them to remote log server in large-scale network. The nxlog is a multi-platform supported and powerful log collection tool, which can easily deploy to collect steadily the log on the target system, and send them to the remote log server with multiple log formats and transmission modes. Moreover, the Syslog as an industrial protocol has been supported by more and more systems. Therefore, based on nxlog and mature log server, the flexible and reliable remote log collection solution can be built easily. The actual operation result shows that this solution can effectively solve the problem of the remote system logs collection in large-scale network.

**Key words:** network security; system log; log collection; nxlog; Syslog; multi-platform

## 0 引言

系统日志文件详细记录系统每天发生的各种各样的事件, 是系统日常运行<sup>[1]</sup>、安全审计<sup>[2]</sup>、取证<sup>[3]</sup>及入侵检测<sup>[4]</sup>的重要资源, 对系统及网络安全具有重要作用<sup>[5]</sup>。因此, 对日志进行安全、有效的管理是非常必要的<sup>[6]</sup>。目前, 将系统日志采集到远程日志管理服务器, 采用远程集中化管理已成为日志管理的普遍共识和有效手段<sup>[7]</sup>。Unix/Linux 系统具有较好的日志管理功能, 可以将日志信息发送到远程日志服务器, 且支持统一的 Syslog 格式<sup>[8]</sup>。但 Windows 平台及其上的

各种应用系统的日志管理功能则相对较弱。日志默认存储在本地, 且各系统的日志格式不统一。这给日志的收集、管理带来了不少困难。虽然已有不少文献从不同角度对类 Unix 平台及 Windows 平台<sup>[4,9]</sup>的日志管理进行了研究, 但面向多个操作系统平台构建完整统一的远程日志采集方案的成果还较少。

nxlog 是一个开源的日志收集管理软件, 部署方便, 功能强大, 支持多种系统平台<sup>[10]</sup>。但目前基于该软件的应用研究还较少。文中简述了类 Unix 平台及 Windows 平台各自支持的日志功能情况, 并详细介绍

收稿日期: 2013-10-08

修回日期: 2014-01-11

网络出版时间: 2014-04-24

基金项目: 河南省科技攻关计划项目(122102310474); 驻马店市科技发展计划项目(11314)

作者简介: 杨锋英(1979-), 女, 研究方向为云计算、计算机网络、智能计算。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20140424.0842.090.html>

nxlog 软件的功能特性、处理架构和内建语言等。基于 nxlog 软件并借助成熟的日志服务器系统,构建了一套稳定可靠的面向多平台的远程日志采集系统。实际运行情况验证了该方案的有效性。

## 1 系统日志简述

### 1.1 类 Unix 系统日志

类 Unix 系统指各种传统的 Unix 系统以及各种与传统 Unix 类似的系统,指代范围非常广泛。此处主要指可以运行在各种主机上的 Unix、Linux 及 Mac OS 等系统。在类 Unix 系统中,有三个主要的日志子系统<sup>[5]</sup>。

连接时间日志:由多个程序执行,把记录写入到/var/log/wtmp 和/var/run/utmp 文件。utmp 文件记录当前登录用户的信息,wtmp 存放用户的登入和退出信息,最后一次登录信息存放在 lastlog 文件中。

进程统计:由系统内核执行。进程统计的目的是为系统中的基本服务提供命令使用统计。

错误日志:由 Syslogd 执行,各种系统守护进程、用户程序和内核通过 Syslog 向文件/var/log/messages 报告值得注意的事件。日志进程 Syslogd 的配置文件是/etc/syslog.conf。可通过配置文件确定记录日志的内容,日志输出的位置(本地文件或远程设备)等。Syslogd 既可记录本地事件,也可通过网络记录另一个主机上的事件。

### 1.2 Windows 系统日志

日志文件是 Windows 系统中一个比较特殊的文件,它记录着 Windows 系统中所发生的各种事件,如用户登录审核、各种系统服务的启动、关闭等信息<sup>[11]</sup>。和 Windows 系统密切相关的日志有应用程序日志、安全日志和系统日志,各自对应的文件名为 AppEvent. evt(x)、SecEvent. evt(x) 和 SysEvent. evt(x),并受到 Event Log(事件记录)服务的保护。

Windows 的日志文件由文件头、日志记录和文件尾三部分构成。文件头和文件尾主要用于标识日志文件的开始和结束,并指示日志记录的数量及位置。日志事件记录由 \_EVENTLOG\_RECORD 结构体类型定义,详细定义了记录大小、记录号、事件时间、事件类型、消息量等信息。

### 1.3 应用系统日志

#### 1) IIS 日志。

IIS 提供 6 种不同的日志格式用于跟踪和分析 IIS 平台下各种站点或服务的信息<sup>[2]</sup>。IIS 的 WWW 日志文件默认位置为 %systemroot%\system32\Logfiles\W3SVC\,用户可自定义日志文件的存放位置。较常用的 IIS 日志格式有 3 种,分别是<sup>[12]</sup>:

(1) W3C Extended Log File Format:是 IIS 服务的默认日志记录格式。信息记录在 ASCII 文本文件中。用户可以选择需要跟踪的字段内容。这种格式包括某些仅适用于 Web 和文件传输协议 (FTP) 服务的字段选项。

(2) NCSA Common Log File Format:一种固定的 ASCII 格式,仅适用于网站。它记录有关用户请求的基本信息,例如远程主机名、用户名、日期时间、请求类型、HTTP 状态码以及服务器发送的字节数等。各项之间用空格分开。

(3) IIS Log File Format:是一种固定的 ASCII 格式。与 NCSA 公用格式相比,它记录的信息项更多,包括一些如所用时间、发送的字节数、操作等详细信息。日志项用逗号分开,更便于用户阅读。

#### 2) Apache 日志。

Apache 服务器会生成两个日志文件<sup>[8]</sup>,即访问日志(access\_log)和错误日志(error\_log)。它们默认存放在 /usr/local/apache/logs 目录下。访问日志记录了所有对 Web 服务器的访问活动,包括远程机器地址、访问的资源、浏览时间及使用的浏览器等。其格式可在 httpd.conf 配置文件中由 LogFormat 命令指定,存储位置可由 CustomLog 命令指定。

错误日志记录了服务器运行期间遇到的各种错误,以及一些普通的诊断信息。可以通过 LogLevel 指令设置记录信息的级别,控制记录信息的数量和类型。错误日志的存放位置可通过 ErrorLog 指令设置。此外,Apache 进程需要使用 Apache 自带的 rotatelog 程序或其他第三程序实现日志滚动,以防日志文件过大影响系统运行。

### 1.4 Syslog 日志格式

Syslog 是各种类 Unix 系统广泛支持的日志协议,由 RFC3164 和 RFC5424 定义和描述<sup>[1]</sup>。一条完整的 Syslog 日志消息包括三个部分:PRI(优先级)、HEADER(包头)和 MSG(消息)<sup>[13]</sup>。

优先级(Priority)部分位于一条 Syslog 消息数据包的最前端,由“<”和“>”分别表示该部分的开始和结束,在括号中的 Priority 值用 1~3 位十进制数表示,并由消息的 Facility 值和 Severity 值来决定,

Facility 是 0~23 的十进制数,它对应了系统中各种不同功能。Severity 是 0~7 十进制数,依次表示的消息级别为:Emergency、Alert、Critical、Error、Warning、Notice、Informational 和 Debug。

包头(HEADER)部分由时间戳(TIMESTAMP)和主机名(HOSTNAME)的两个域组成。TIMESTAMP 采用的格式是“Mmmddhh:mm:ss”。HOSTNAME 包含主机的名称,若无主机名或无法识别则显示 IP 地址。消

息(MSG)部分通常包含了产生信息进程的额外信息,以及信息的文本部分。没有结束标志,长度可以为 0~1 024 字节。MSG 包含两个域:TAG 和 CONTENT。TAG 域标识产生信息的程序或者进程的名称。CONTENT 包含了信息的详细内容。

2 nxlog 软件系统

2.1 nxlog 概述

nxlog 是一个功能强大的日志收集、管理工具,可以工作在异构环境中收集数百个不同源(如 TCP、UDP、文件、数据库等)和不同格式(如 Syslog、Windows 事件日志及用户自定义格式等)的事件日志<sup>[10]</sup>。还可以执行如日志重写、关联、告警、模式匹配以及日志轮转等任务。nxlog 当前最新版本为 2.5 版,其主要的功能特性如下:

- 1)多平台支持:可运行在各种类 Unix 系统(如 Linux、Mac 等)及各种 Windows 平台上。
- 2)客户/服务器模式:nxlog 既可以充当客户端,从本地文件或操作系统上收集日志然后发送到远程服务器,也可以充当服务器,从网络上接受连接并接收日志,然后把它们写到文件或数据库中。
- 3)模块化架构:具有一个轻量级的模块化架构,可插接具有不同功能特性的模块,如日志格式解析、传输协议处理、数据库处理等。

此外,nxlog 还支持消息缓存、多线程处理、多优先级处理及内嵌语言等功能特性。

2.2 nxlog 处理架构

nxlog 的插件架构通过加载不同的模块可以读取任意类型的输入数据、解析和转换信息的格式并以任意类型输出。不同的输入、处理和输出模块可以同时使用以满足各种日志环境。图 1 展示了基于此架构的日志消息处理流程。

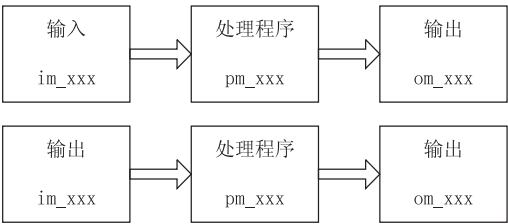


图 1 nxlog 处理架构

nxlog 内核负责解析配置文件、监控文件和 Sockets,并有一个基于事件的架构来管理各种内部事件。所有模块都可以向内核派发事件。内核接管这些事件并任意传递到某个模块来处理。nxlog 也是一个基于多线程的应用,其主线程负责监控文件或 Sockets,并有一个专用的线程处理内部事件。在处理下一个事件前线程处于休眠状态,被唤醒后可以分派事件到工作

者线程(Worker Thread)。工作者线程接收的事件必须立即被处理。这样 nxlog 内核就可以集中控制所有的事件,而且这些事件的执行顺序可以满足优先级处理的要求。

处理文件或 Sockets 的模块使用非阻塞 I/O 方式,可以保证工作者线程不会阻塞。被主线程监控的文件和 Sockets 也可以通过委托的方式分派事件给工作者。属于同一个模块的事件被顺序处理,这保证了消息处理的顺序性,并且不必处理复杂的并发性问题。然而,由于各个模块是并发运行的,因此全局的日志处理流也是并行的。

当输入模块接收到数据时,会创建一个日志消息的内部表示结构。然后这个日志消息根据路由指示被放入下一模块的队列中,并生成一个数据可用的通知信号。输入模块之后的模块通常是处理模块或是输出模块。但输入和输出模块也可以通过内建代码或 nxlog 语言运行框架处理数据。不同的是处理模块运行在其他的工作者线程中,日志处理的并行性更好。而且处理模块可以链接起来,在系统的多个 CPU 或 CPU 内核间分配任务。

2.3 nxlog 内建语言

nxlog 内核内嵌有一个解释语言,可用来编制复杂的决策或者在 nxlog 配置文件中建立表达式。nxlog 语言是一个强类型语言,这可以在解析配置时进行严格的语法检查以确保类型安全。当 nxlog 开始读配置文件时,包含在 nxlog 语言代码中的指令将被解析并编译成伪代码。接着伪代码被提交给运行时评估。由于 nxlog 语言比较简单,没有错误处理功能。如果发现有语法错误,nxlog 将在控制台输出这些错误。

3 基于 nxlog 的远程日志采集方案

在远程日志采集中,一般采用代理/管理者的采集模型。常见的数据采集方式有:SNMP Trap 机制采集、系统日志(Syslog)协议的采集、Telnet 采集及文本方式(mail 或 FTP)采集等<sup>[14]</sup>。其中,基于 Syslog 协议的日志数据采集是最常用的日志采集方式<sup>[1]</sup>。基于 nxlog 软件并配合成熟的日志服务器系统可以方便地构建一个远程日志采集模型,如图 2 所示。

在该模型中,首先需要在采集日志的主机上部署 nxlog 软件,并以后台服务的形式运行。通过修改配置文件,可以指定 nxlog 采集的日志源以及处理方式。nxlog 支持多种日志输出格式,但为了便于日志服务器的处理,可以设定最常用的 syslog 格式作为日志输出格式。nxlog 服务可以根据日志服务器的配置,采用 UDP、TCP、SSL 或 HTTP 作为传输协议将日志发送给远端。日志服务器上运行有 syslog 服务进程,这可由

rsyslog 或 syslog-ng 的软件系统提供, nxlog 本身也可以构建日志服务器。日志服务器在接收到日志信息之后, 要依据预配置的策略, 对日志进行必要的预处理, 然后存储到本地文件、数据库或云存储设备中。

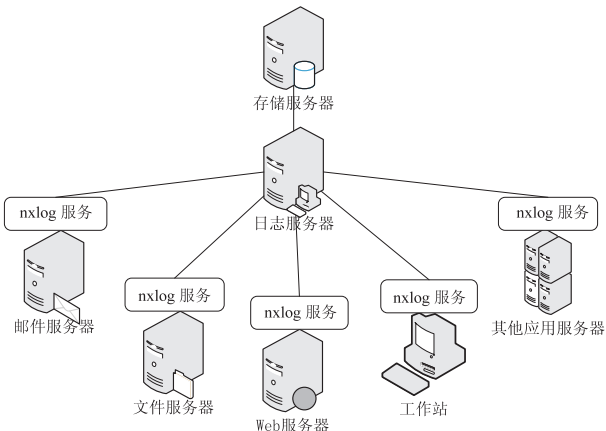


图 2 基于 nxlog 的日志采集模型

## 4 系统实现

为验证基于 nxlog 的远程日志采集系统的可用性, 此处构建了一个由 4 台主机构建的小型环境。其中三台充当日志源, 分别提供 Windows、Linux 和 IIS 日志信息。另一台主机充当日志服务器。为了简化实验过程, 此处仅列出最基本的配置。

### 4.1 系统配置

nxlog 软件的安装过程都非常简单, 不再赘述。安装完成后需要对配置文件 nxlog.conf 进行必要的配置。在 Windows 平台上配置文件位于 nxlog 安装目录下的 conf 子目录中。Linux 平台中可以在 /etc/ 目录中找到该文件。配置文件中已经预置了一些配置项, 不同平台下配置略有不同。

在 Windows 平台下, 配置文件中的 ROOT 指令符需要按软件的实际安装位置进行修改, 如下:

```
define ROOT C:\Program Files\nxlog
```

接着配置系统的输入模块, 若是 Windows2003 以前的版本需要使用 im\_mseventlog 模块, 否则保持默认的 im\_msvistalog 模块即可。此外, Windows 平台的日志信息多采用 UTF-16 格式, 可以转化成 UTF-8 格式。输入模块配置如下所示:

```
<Input in>
```

```
Module im_msvistalog
```

```
Exec convert_fields('UTF-16','UTF-8');
```

```
</Input>
```

Linux 平台下, 可以先定义 BASEDIR 指示符如下:

```
define BASEDIR /var/log
```

然后配置系统的输入模块如下:

```
<Input in>
```

```
Module im_file
```

```
File '%BASEDIR%/messages'
```

```
</Input>
```

不同平台的输出模块配置相近, 需要选择日志的传输协议、日志服务器地址及端口号等信息。通常 syslog 服务以 UDP 协议并使用 514 端口, 可以配置如下:

```
<Output out>
```

```
Module om_udp
```

```
Host 192.168.0.1(参考实际情况设置)
```

```
Port 514
```

```
</Output>
```

配置完成后, 在各自平台上启动 nxlog 服务即可。

### 4.2 日志收集及显示

在日志服务器端开启日志服务进程。在打开的日志显示窗口中, 可以看到收集的远程系统的日志信息。这说明基于 nxlog 软件构建面向多平台的远程日志收集系统是可行的。而且整个部署过程非常便捷、灵活。

## 5 结束语

系统日志是系统安全管理的重要资源。由于多平台环境下各系统的日志格式较多, 很难将大型网络中各系统的事件日志收集、整合到远程日志服务器上。nxlog 是一款功能强大的日志收集、管理工具, 可以有效解决多平台系统上的日志收集问题。结合成熟的日志服务器, 可以形成一套灵活、高效的远程日志采集方案。实际运行效果验证了方案的可行性。

### 参考文献:

- [1] 顾清. 基于日志采集的分布式网管系统设计与实现[D]. 上海: 上海交通大学, 2008.
- [2] 杨尚大. 日志数据采集和实时审计关键技术研究[EB/OL]. 杭州: 浙江工商大学, 2009.
- [3] 林英, 张雁, 欧阳佳. 日志检测技术在计算机取证中的应用[J]. 计算机技术与发展, 2010, 20(6): 254-256.
- [4] 雷惊鹏, 颜世波. 基于 Windows 日志的主机入侵检测[J]. 吉林工程技术师范学院学报, 2013, 29(1): 71-72.
- [5] 张婕, 张大力, 李文祯. 网络和系统的日志采集及分析[J]. 计算机工程, 2000, 26(S): 356-360.
- [6] Kent K. Guide to computer security log management[EB/OL]. (2006-05-01)[2007-08-12]. <http://esrc.nist.gov/publications/nistpubs/800-92/SP80-92.pdf>.
- [7] 肖诗松, 陈涛. 基于插件技术的日志采集 Agent 系统的设计与实现[J]. 东南大学学报(自然科学版), 2008, 38(S): 90-93.
- [8] 张传立. 基于 Linux 的日志分析[J]. 科技信息, 2011(13): 55-56.
- [9] 王春彦, 朱磊, 杨晓朋. 基于 Windows 的 Syslog 日志系统设计与实现[J]. 微型机与应用, 2012, 31(4): 11-13.

(下转第 156 页)

表 1 噪声大小比较

实际噪声	文献[8]	文中算法
0.010	0.009 7	0.009 8
0.050	0.046 0	0.049 0
0.100	0.092 0	0.094 0
0.150	0.143 0	0.146 0
0.200	0.160 0	0.180 0

表 2 观测值不同时噪声大小比较

实际噪声大小	观测值个数	文中算法
$j=0.01$	$n=10$	0.008 5
	$n=20$	0.009 1
	$n=30$	0.009 4
	$n=40$	0.009 7
	$n=50$	0.009 8
$j=0.05$	$n=10$	0.043 0
	$n=20$	0.045 0
	$n=30$	0.046 0
	$n=40$	0.048 0
	$n=50$	0.049 0
$j=0.10$	$n=10$	0.086 0
	$n=20$	0.089 0
	$n=30$	0.091 0
	$n=40$	0.092 0
	$n=50$	0.094 0
$j=0.15$	$n=10$	0.136 0
	$n=20$	0.141 0
	$n=30$	0.143 0
	$n=40$	0.144 0
	$n=50$	0.146 0
$j=0.20$	$n=10$	0.110 0
	$n=20$	0.130 0
	$n=30$	0.140 0
	$n=40$	0.160 0
	$n=50$	0.180 0

从实验结果中可以得出以下结论:从表 1 的文中算法与实际噪声值比较接近,能够比较正确地估计噪声图像的噪声值的大小。同时,从表 2 中取不同个数观测值所得噪声值进行对比,表明所取样本的个数越大,则对噪声值估计越准确。

3 结束语

文中只是针对图像含有较小的高斯噪声进行有效的估计,方法简单,易于实现,在今后的研究中还需要重点解决以下几个问题:对其他噪声此方法是否适用;图像噪声估计与去除噪声算法两者结合的研究;混合噪声的去除方法。

参考文献:

[1] Spann M, Wilson R. A quad-tree approach to image segmentation which combines statistical and spatial information[J]. Pattern Recognition, 1985, 18(3-4): 257-269.

[2] 顾晓东, 郭仕德, 余道衡. 一种基于 PCNN 的图像去噪新方法[J]. 电子与信息学报, 2002, 24(10): 1304-1309.

[3] Gilboa G, Sochen N, Zeevi Y Y. Estimation of optimal PDE-based denoising in the SNR sense[J]. IEEE Trans on Image Processing, 2006, 15(8): 2269-2280.

[4] 李万臣, 赵开伟. 基于中值滤波和 Contourlet 变换的图像去噪研究[J]. 哈尔滨商业大学学报(自然科学版), 2011, 27(2): 211-214.

[5] 张旗, 梁德群, 樊鑫. 基于小波域的图像噪声估计新方法[J]. 计算机工程, 2004, 30(8): 37-39.

[6] 张旗, 梁德群, 樊鑫, 等. 基于小波域的图像噪声类型识别与估计[J]. 红外与毫米波学报, 2004, 23(4): 281-285.

[7] Amer A, Dubois E. Fast and reliable structure-oriented video noise estimation[J]. IEEE Trans on Circuits and Systems for Video Technology, 2005, 15(1): 113-118.

[8] 赖施成, 贾洞. 基于块内邻域相关度的图像噪声估计[J]. 计算机与现代化, 2009(12): 82-84.

[9] Olsen S I. Estimation of noise in images: an evaluation[J]. Graphical Models and Image Processing, 1993, 55(4): 319-323.

[10] 张旭升, 周桃庚, 沙定国. 数字图像噪声估计的方法及数学模型[J]. 光学技术, 2005, 31(5): 719-722.

[11] 李俊山, 李旭辉. 数字图像处理[M]. 北京: 清华大学出版社, 2007.

[12] Gonzalez R C, Woods R E. 数字图像处理[M]. 第 3 版. 北京: 电子工业出版社, 2012.

[13] 张国权. 应用概率统计[M]. 北京: 科学出版社, 2006.

[14] 张德丰. 数字图像处理[M]. MATLAB 版. 北京: 人民邮电出版社, 2009.

(上接第 152 页)


[10] NXLOG community edition reference manual for v2. 5. 1089 [EB/OL]. 2009-12-15. <http://www.nxlog.org/nxlog-docs/en/nxlog-reference-manual.html>.

[11] 刘秀波, 王连海. Windows XP 日志文件格式分析[J]. 软件导刊, 2011, 10(1): 36-38.

[12] Logfile formats in IIS [EB/OL]. 2013-10-01. [\[brary/IIS/bea506fd-38bc-4850-a4fb-e3a0379d321f.mspx?mfr=true\]\(http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/bea506fd-38bc-4850-a4fb-e3a0379d321f.mspx?mfr=true\).

\[13\] 谢长华. Syslog 日志高效解析和异常检测\[D\]. 西安: 西安电子科技大学, 2007.

\[14\] 刘必雄, 魏连, 许榕生. 基于 Agent 技术的多源日志采集系统的设计与实现\[J\]. 计算机系统应用, 2008\(2\): 71-74.](http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Li-</a></p></div><div data-bbox=)

作者: 杨锋英, 刘会超, YANG Feng-ying, LIU Hui-chao  
作者单位: 杨锋英, YANG Feng-ying(黄淮学院 信息工程学院, 河南 驻马店, 463000), 刘会超, LIU Hui-chao(黄淮学院 信息工程学院, 河南 驻马店463000; 武汉大学 计算机学院, 湖北 武汉430072)  
刊名: 计算机技术与发展   
英文刊名: Computer Technology and Development  
年, 卷(期): 2014(7)

参考文献(14条)

1. 顾清 基于日志采集的分布式网管系统设计与实现 2008  
2. 杨尚大 日志数据采集和实时审计关键技术研究 2009  
3. 林英;张雁;欧阳佳 日志检测技术在计算机取证中的应用 2010(06)  
4. 雷惊鹏;颜世波 基于Windows日志的主机入侵检测 2013(01)  
5. 张婕;张大力;李文祯 网络和系统的日志采集及分析 2000(S)  
6. Kent K Guide to computer security log management 2007  
7. 肖诗松;陈涛 基于插件技术的日志采集Agent系统的设计与实现 2008(S)  
8. 张传立 基于Linux的日志分析 2011(13)  
9. 王春彦;朱磊;杨晓朋 基于Windows的Syslog日志系统设计与实现 2012(04)  
10. NXLOG community edition reference manual for v2. 5. 1089 2009  
11. 刘秀波;王连海 Windows XP日志文件格式分析 2011(01)  
12. Logfile formats in IIS 2013  
13. 谢长华 Syslog日志高效解析和异常检测 2007  
14. 刘必雄;魏连;许榕生 基于Agent技术的多源日志采集系统的设计与实现 2008(02)

引用本文格式: 杨锋英, 刘会超, YANG Feng-ying, LIU Hui-chao 面向多平台的日志远程采集系统研究[期刊论文]-  
计算机技术与发展 2014(7)