Software Engineering and Applications 软件工程与应用, 2016, 5(4), 254-258
Published Online August 2016 in Hans. http://www.hanspub.org/journal/sea
http://dx.doi.org/10.12677/sea.2016.54029

Hans汉斯

The Application of Centralized Management Log Server in Network Management

Cunliang Pan, Yanling Yang

Hami Regional Meteorological Bureau, Hami Xinjiang
Email: pancl@126.com

Received: Aug. 8th, 2016; accepted: Aug. 27th, 2016; published: Aug. 30th, 2016

Abstract

Logs can accurately and timely record the operation situation of the network and servers. They are the focus of network management personnel. This paper discusses the construction of the centralized management log server, as well as the application in the management of the communication network.

Keywords

Log Server, Centralized Management, Collection, Analysis

集中管理日志服务器在网络管理中的应用

潘存良，杨艳玲

哈密地区气象局，新疆 哈密
Email: pancl@126.com

收稿日期：2016年8月8日；录用日期：2016年8月27日；发布日期：2016年8月30日

摘　要

日志能准确及时记录网络、服务器运行情况，是网络管理人员重点关注对象。本文论述了集中管理日志服务器的搭建，以及在通信网络管理中的应用。

文章引用: 潘存良，杨艳玲. 集中管理日志服务器在网络管理中的应用[J]. 软件工程与应用, 2016, 5(4): 254-258.
http://dx.doi.org/10.12677/sea.2016.54029

关键词

日志服务器，集中管理，采集，分析

1. 引言

日志是设备对于发生事件的记录。它记录了系统每天发生的各种事件，维护人员可以通过它来检查设备的运行情况。服务器、网络设备、安全设备每天都在产生大量的日志，这些日志记录了设备的运行情况，用户对设备的访问操作，我们可以根据这些日志监控网络的运行情况，及时发现一些异常事件。这些日志默认分布在设备自身的日志文件或日志缓存中，信息量大且极为复杂。在日常网络管理中查看设备、服务器日志就带有很大盲目性，其工作量也非日常管理维护可以顺利承担的，及有可能错漏一些重要事件的日志，耽误解决问题的时间和机会。随着网络应用的快速发展，日志数量也急剧增加，如何对其进行有效的管理，成为了迫切需要解决的问题。建立集中管理的中央日志服务器，就是有效解决日志管理的方法。

2. 系统日志(Syslog)协议简介

系统日志(Syslog)协议是在 IP 网络中转发系统日志信息的工业标准。在网络管理领域，Syslog 协议提供了一种信息传递方式，允许一个设备通过网络把事件信息传递给事件信息接收者。

Syslog 消息格式：FACILITY-SUBFACILITY-SEVERITY-MNEMONIC：Message-text

Facility(特性)：由 2 个或 2 个以上大写字母组成的代码，用来表示硬件设备、协议或系统软件的型号。

Severity(严重性)：范围为 0~7 的数字编码，表示了事件的严重程度。

Mnemonic(助记码)：唯一标识出错误消息的代码。

Message-text(消息文本)：用于描述事件的文本串。消息中的这一部分有时会包含事件的细节信息，其中包括目的端口号、网络地址或系统内存地址空间中所对应的的地址。

3. 集中管理日志服务器的搭建

集中管理日志服务器利用 Syslog 协议实现日志信息的接收与传递，是一套软硬结合的系统，为了确保日志数据的安全，需要专门的服务器，服务器对存储空间有较大的要求，对其他硬件要求不高[1]，目前条件很容易满足。

经过测试和比较，选用 Suse Linux 11 sp3 作为日志服务的系统服务平台，使用其自带的 Syslog-ng 作为日志系统服务端，将日志存储在 mysql 数据库中，通过 Logzilla 这个 Syslog 和其他网络事件数据 Web 前端显示工具，提供简单易用的日志浏览、搜索和基本分析以及图表显示等功能。由于整个系统对系统时间及网络端口有一致性的要求，各日志输出端都需设置时间服务器，进行时间同步，并在防火墙上开通相应端口。

3.1. 系统结构

系统采用 Syslog-ng 作为集中日志服务端，日志数据存放到 mysql 数据库中，通过 Web 方式浏览、分析集中收集的日志信息。具体系统构架如图 1 所示。

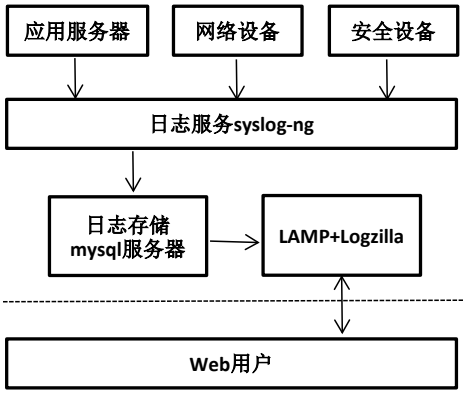

Figure 1. Centralized management log service system structure
图 1. 集中管理日志服务系统结构

3.2. 日志服务器端的建立与日志数据接收

3.2.1. 建立日志服务配置 syslog-ng，接收日志并写入 mysql 数据库

1) 首先建立相应的数据库和表，用来存放服务端收到的日志信息，脚本如下：

```
CREATE DATABASE syslog;
USE syslog;
CREATE TABLE logs (
host varchar(32) default NULL,
facility varchar(10) default NULL,
priority varchar(10) default NULL,
level varchar(10) default NULL,
tag varchar(10) default NULL,
date date default NULL,
time time default NULL,
program varchar(15) default NULL,
msg text,
seq int(10) unsigned NOT NULL auto_increment
) ENGINE=myisam；
```

2) syslog-ng 配置说明

Syslog-ng 的主配置文件存放在：/etc/syslog-ng/syslog-ng.conf。一般都会含有以下 5 段。

Options｛｝段，用来进行全局设置。典型的全局选项如下：

```
options {
        Sync(0);
        log_fifo_size(2048);
        create_dirs(yes);
        create_dirs(yes);
        group(logs);
        dir_group(logs);
```

```
        perm(0640);
        dir_perm(0750);
};
```

source｛｝段定义日志信息来源，可以是 file、unix-stream、udp、tcp、pipe 或 fifo 中的一个或多个，下例就是一个可以从 tcp、udp 的 514 端口获取消息的信息源。

```
source s_src {
        tcp(ip(0.0.0.0) port(514));
        udp(ip(0.0.0.0) port(514));
};
```

filter｛｝段定义日志的过滤器。在日志产生过程中，一些普通事件或特定服务的日志无需将输出，则可通过过滤器剔除，在过滤器中可以使用正则表达式，还可以包括逻辑操作符。下例就是一个监听 x.x.x.x 主机的日志消息，当出现消息为"Denial of Service"时工作。

```
filter firewall_filter { host("x.x.x.x") and match("Denial of Service"value("MESSAGE")); };
```

destination{}段定义服务器收到信息后怎样处理。日志消息可以写入指定文件、发送到指定 tcp 端口、发送到指定管道 fifo 设备或启动指定程序处理日志消息。下例就是启动 mysql 程序，将日志消息处理，写入数据库中。

```
destination d_mysql {
    program("/usr/bin/mysql -usyslogadmin -psyslogadmin syslog"
    template("INSERT INTO logs (host, facility, priority, level, tag, fo, program, msg, seq) VALUES( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL', '$TAG', '$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC', '$PROGRAM', '$MSG', '$SEQ' );\n")
    template-escape(yes));
};
```

Log｛｝段定义消息的路径，就是把日志信息的信息源、过滤器、信息目的组合起来形成一条完整的指令。消息路径中的成员是按顺序执行的，来源于指定的消息源，匹配所有过滤器，并送到指定目的。在 log｛｝段，过滤器不是必须的。下例就是一个标准的消息路径。

```
log {
        source(s_src);
        filter(firewall_filter);
        destination(d_mysql);
};
```

在配置文件中除 options｛｝段外，其他几段都可以重复定义。

3.2.2. Windows 系统日志入库

Windows 系统有自己的日志协议，称为 Event Log。我们使用 evtsys 软件将 windows 系统的日志发送的 Syslog-ng 服务器上，evtsys 可网上下载其 32 或 64 位版本。将下载的 evtsys.dll 和 evtsys.exe 拷贝到系统的 c:\windows\system32 目录下。以管理员身份执行如下命令

```
Evtsys -i -h 172.23.192.3 -p 514
net start evtsys
```

打开组策略编辑器(gpedit.msc)，在 windows 设置－> 安全设置 －> 本地策略 －>审核策略 中，打

开你需要记录的 windows 日志。evtsys 会实时的判断是否有新的 windows 日志产生，然后把新产生的日志转换成 syslog 可识别的格式，发送到 syslog 日志服务端[2]。

3.2.3. 博达路由器日志

如下配置路由器，定义日志生成等级，使其生成的日志发送到日志服务器上

Logging facility local7

logging host 172.23.192.3

Logging start

3.3. Logzilla 日志 Web 客户端

Logzilla2.99 版是一款免费的集日志浏览、搜索和分析以及图表显示等功能为一体的 Web 前端软件。将下载的软件解压到 apache 服务器的 httpdocs 目录下，配置 apache 服务，建立相应的虚拟目录。通过浏览 http://172.23.192.3/logs/ 根据提示完成安装。安装完成后可通过浏览 http://172.23.192.3/logs/查看集中收集的日志，并分析日志。

4. 集中管理日志服务在网络管理中的应用

集中存储在日志服务器中的数据，既可以在日常网络管理中查阅，也可以对其数据进行挖掘分析。

通过对日志信息的查阅了解，可全面监控网络运行情况，及时发现可能存在的安全事件或网络故障，及时做出响应。主动查看日志信息能有利于用户更好的发现潜在的威胁，提高设备服务的效率，及时化解安全危机。

通过对日志数据的统计分析，能很好的发现设备、服务的运行规律，总结出网络设备负载及资源利用情况，也可以反映网络安全情况，发现网络攻击时间，来源，目标等信息，根据这些信息改善网络性能，优化资源配置。

5. 结束语

通过对集中管理日志服务器建设方法的研究，完成日志集中采集入库，并通过 Web 方式显示分析应用，提供日志数据集中存储管理利用的一种思路和方法。

参考文献 (References)

[1] 陈庭平, 沈丽娟, 曾鹏. 日志服务器建设和应用[J]. 网络安全技术与应用, 2010(9): 65-68.

[2] 吕荣峰. 基于 syslog-ng 的集中式日志服务器及其客户端配置方法[J]. 数字技术与应用, 2014(4): 168-169.