基于 Windows 的 Syslog 日志系统设计与实现

王春彦[1]，朱 磊[2]，杨晓朋[2]
（1. 河南省电子产品质量监督检验所，河南 郑州 450003；
2. 河南省电力通信自动化公司，河南 郑州 450052）

摘 要：针对传统的单一设备和人工管理方式不能应对日益复杂的网络威胁和挑战，不能及时发现和准确定位网络安全事件，也不能对安全事件可能造成的后果进行准确评估的问题，本文主要讨论如何基于标准 Syslog 协议，通过对网络设备大量网络日志数据的集中采集，通过 SQL 代理处理后进行分析，构造一套日志系统，以达到对网络运行状况进行检测的目的。

关键词：Syslog；日志系统；SQL 代理；网络安全
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1674-7720(2012)04-0011-03

Windows-based system design and implementation of Syslog

Wang Chunyan[1], Zhu Lei[2], Yang Xiaopeng[2]
(1. Henan Electronic Product Quality Supervision and Inspection, Zhengzhou 450003, China;
2. Henan Electric Power Communication & Automation Company, Zhengzhou 450052, China)

Abstract: The traditional reliance on a single device, or manual management approaches have failed to respond to increasingly complex challenges of network threats and can not find and accurately locate the network security incidents, security incidents can not be an accurate assessment of the consequences. This article focuses on how standards-based syslog protocol, a large number of network devices through the network of a centralized collection of log data, processed by the SQL Agent to analyze, construct a log system to achieve operational status of the network for testing purposes.

Key words: Syslog; log system; SQL agent; network security

日志一直都是网络管理人员在检查故障、排除网络错误时，查找“病源”的有利原始资料。通过对网络设备和主机系统的日志分析，可以快速了解网络上的活动，并对刚刚发生的或者正在进行的事件进行快速响应。随着网络规模的不断扩大和网络应用的不断增多，网络中也越来越多地面临各种安全威胁的困扰，传统的依靠单一设备或者人工管理的方式已不能应对日益复杂的网络威胁的挑战，不能及时发现和准确定位网络安全事件，也不能对安全事件可能造成的后果进行准确评估。

1 Syslog 协议简述

Syslog 是一种工业标准协议，可用来记录设备的日志。在 Unix 系统的路由器、交换机等网络设备中，Syslog 记录系统中的任何事件，管理者可以通过查看系统记录，随时掌握系统状况。除了可以把日志信息保存在日志文件中之外，Syslog 协议还允许设备把日志信息通过网络传递给日志服务器[1]。

2 日志采集和存储

现在大多数 Syslog 日志系统均采用 Linux 服务器，针对某企业的设备情况，这里建设一套 Windows 下的日志系统[2]，本文采用 Kiwisyslog 日志采集软件来收集需要的系统日志，Kiwisyslog 遵循标准的日志协议(RFC 3164)，并支持 UDP/TCP/SNMP 几种方式的日志输入，且它自带发送模拟器、日志浏览器等实用工具。

对于 Kiwisyslog 收集到的日志，选择实时存入数据库 syslogd，日志格式如图 1 所示。

图 1 日志格式

由于本企业上网用户超过 3 000 人，每天日志量非常庞大。在这个日志内容中，主要对 Message 字段进行分析，但是此字段内容较多且复杂，后期的日志统计分析非常困难，这里采用对 syslogd 数据库进行每天作业处

理，将 Message 字段按照规律进行字段划分，Message_A 字段是日志类型，Message_B 字段是访问时间，Message_C 字段是源地址和目的地址，Message_D 和 Message_E 字段是流入和流出流量，结果如图 2 所示。

图 2 Message 字段分析结果

具体操作如下：

打开 SQL 企业管理器，进入服务器名下的“管理”，启动 SQL Server 代理。然后查看服务器属性，选中“自动启动 SQL Server 代理”。

接下来进入 SQL Server 代理下的“作业”，在右边点右键选“新建作业”。

在“常规”里，输入一个作业名“syslogd 每日处理”，分类选最后一项“数据库维护”。

在“步骤”里，点“新建步骤”，随便输入一个步骤名如“每日备份”，数据库选 syslogd，命令里输入需要处理的 SQL 语句，之后分析一下，没有问题再继续添加下一个。在“高级”里将“失败时的操作”改成“转到下一步”。

在“调度”里，点“新建调度”，随便输入一个调度名，点“更改”，“发生频率”选每天，“一次发生于”里设置 00:00:01，然后点“确定”，再点“确定”，配置完成。详细 SQL 语句如下[3]：

(1) 日志备份

```
--获取昨日日期形成日期字符串
declare @tbName varchar(100),@sql varchar(2000),@date datetime
select @tbName = convert(varchar(10),getdate()-1,112)
--修改表 syslogd 表名为日期字符串名字
EXEC sp_rename 'syslogd',@tbName
--删除三个月前的表
select @date=dateadd(month,-3,getdate())
declare cur cursor for select name from sysobjects where crdate<@date and xtype='U'
open cur
fetch next from cur into @tbName
while @@fetch_status=0
    begin
        select @sql='drop table '+@tbName
        exec(@sql)
        fetch next from cur into @tbName
    end
        close cur
        deallocate cur
--生成新的 syslogd 数据表并创建索引
    if exists (select * from dbo.sysobjects where id = object_id (N'[dbo].[syslogd]') and OBJECTPROPERTY (id, N'IsUserTable') = 1)
    drop table [dbo].[syslogd]
    GO
    CREATE TABLE [dbo].[syslogd] (
        [MsgDate] [varchar] (10) COLLATE Chinese_PRC_CI_AS NOT NULL,
        [MsgTime] [varchar] (8) COLLATE Chinese_PRC_CI_AS NOT NULL ,
        [MsgPriority] [varchar] (50) COLLATE Chinese_PRC_CI_AS NULL ,
        [MsgHostname][varchar] (255) COLLATE Chinese_PRC_CI_AS NULL,
        [MsgText] [varchar] (900) COLLATE Chinese_PRC_CI_AS NOT NULL
    ) ON [PRIMARY]
    GO
    CREATE INDEX [IX_syslogd] ON [dbo].[syslogd]([MsgText]) ON [PRIMARY]
    GO
```

(2) 划分字段

```
    if exists (select * from dbo.sysobjects where id = object_id (N'[dbo].[f_GetStr]') and xtype in (N'FN', N'IF', N'TF'))
    drop function [dbo].[f_GetStr]
    GO
    --分段截取函数
    CREATE FUNCTION dbo.f_GetStr(
    @s varchar(8000),      --包含多个数据项的字符串
    @pos int,              --要获取的数据项的位置
    @split varchar(10)     --数据分隔符
    )RETURNS varchar(100)
    AS
    BEGIN
        IF @s IS NULL RETURN(NULL)
        DECLARE @splitlen int
        SELECT @splitlen=LEN(@split+'a')-2
        WHILE @pos>1 AND CHARINDEX(@split,@s+@split)>0
            SELECT @pos=@pos-1,
                @s=STUFF(@s,1,CHARINDEX(@split,@s+@split)+@splitlen,'')
            RETURN (ISNULL (LEFT (@s,CHARINDEX (@split,@s +@split)-1),''))
    END
    GO
    --获取昨日日期形成日期字符串
    declare @tbName varchar (100),@sql varchar(2000),@date datetime
    select @tbName = convert(varchar(10),getdate()-1,112)
    select @sql='select MsgDate, MsgTime,
        dbo.f_GetStr([MsgText],1,"") MsgText_A,
```

```
        dbo.f_GetStr([MsgText],2,"") MsgText_B,
        dbo.f_GetStr([MsgText],3,"") MsgText_C,
        dbo.f_GetStr([MsgText],4,"") MsgText_D,
        dbo.f_GetStr([MsgText],5,"") MsgText_E,
        dbo.f_GetStr([MsgText],6,"") MsgText_F
    into syslogd_'+@tbName+' FROM'+quotename(@tbName)
    exec(@sql)
    --在新表的 MsgText_C 字段建立索引
    exec('CREATE INDEX [IX_syslogd] ON [dbo].[syslogd_'
+@tbName+'](MsgText_C]) ON [PRIMARY]')
    GO
```

(3) 日志筛选

```
    --获取昨日日期形成日期字符串
    declare @tbName varchar (100),@sql varchar(2000),@date
datetime
    select @tbName = convert(varchar(10),getdate()-1,112)
    --获取昨日 http 日志存入 log_http_ 昨日日期日志库
    select @sql='select * into log_http_'+@tbName+'FROM
syslogd_'+@tbName+'where MsgText_C ="get"or MsgText_C="
post"'
    exec(@sql)
    exec('CREATE INDEX [IX_syslogd] ON [dbo].[log_http_'
+@tbName+'](MsgText_D]) ON [PRIMARY]')
    GO
```

(4) 其他类型日志

按照以上方法同样可以获取 session 日志、qq 日志、msn 日志等。

(5) 删除无用数据表

```
    declare @tbName varchar (100),@sql varchar(2000),@date
datetime
    select @tbName = convert(varchar(10),getdate()-1,112)
    --删除 1 天前的 syslogd_2010xxxx 表
    select @sql='drop table syslogd_'+@tbName
    exec(@sql)
```

3 日志分析

通过系统采集的日志，可选择不同的日期或日期区间进行日志检索并进行分析。通过 C# 语言开发查询工具，查询界面如图 3 所示。

图 3 查询界面

查询工具的关键代码如下[4]：

```
    string sql = "";
DateTime dtbegin = dateTimePicker1.Value;    //开始时间
DateTime dtend = dateTimePicker2.Value;      //结束时间
if (this.comboBoxTableName.Text.Contains("http"))
                                    //查询 log_http_2010xxxx
    {
        while ((dtend-dtbegin ).Days >= 0)
        {
            string dbtablename="log_"+comboBoxTable-
            Name.Text + "_" + dtbegin.ToString("yyyy
            MMdd");
            if (sql == "")
                sql="select MsgDate as 日期,MsgTime
                as 时间,MsgText_B as 源 IP,MsgText_
                C as 访问方式,MsgText_D as 目的网
                址 from"+dbtablename;
            else
                sql = sql + " union all select MsgDate
            as 日期,MsgTime as 时间,MsgText_B as
            源 IP,MsgText_C as 访问方式,MsgText_D
            as 目的网址 from " + dbtablename;
            if (this.checkBoxText.Checked)
                sql = sql + " where MsgText_D like
                '%" + this.textBoxMsgText.Text + "%
                'or MsgText_B like '%" + this.
                textBoxMsgText.Text + "%'";
            dtbegin = dtbegin.AddDays(1);
        }
    }
```

通过日志查询工具，输入日志服务器 IP、数据库名和登录信息，点击连接数据库，连接无误后即可选择日志类型、开始及结束日期，可以查询某一时间段内相关关键字的所有日志，并可以选择导出记录到 Excel，达到详细分析的目的。

本文在对网络设备日志分析的基础上为网络管理提供了一种较为简单的方法，但这些研究与实现只是一些基础性工作，在该架构和基础上还可以做进一步开发，为企业提供更多的便利：(1)网络计费是网络管理中的一个重要环节，利用本文提供的准确的进出口流量数据，配合计费策略信息库，可以构建比较完善的网络计费系统。(2)目前用户行为分析是企业关注的一项课题，可以利用建立的部分 IP 地址同域名的对照关系以及建立 URL 与网页内容关键字的映射关系，分析出用户的兴趣爱好。

参考文献

[1] 张永生，谭成翔，汪海航.Linux 环境下构建安全的日志服务器[J].计算机安全，2006(12):6-8.

[2] 刘合富. syslog 日志数据采集实现[J]. 中国网络教育, 2007(8):50-51.
[3] 郑阿奇.SQL SERVER 实用教程[M].北京:电子工业出版社,2005:261-282.
[4] CSDN 社区 [EB/OL].(2010-04-28).http://topic.csdn.net/u/20100428/22/64b61824-973b-4acd-b420-3bbe39793b65.html.

(收稿日期:2011-11-28)

作者简介:

王春彦,女,1982 年生,助理工程师,学士,主要研究方向:软件开发、软件测试、信息化建设。

朱磊,男,1983 年生,助理工程师,学士,主要研究方向:IP 网络、ASP.NET WEB 工程、信息化运维。

杨晓朋,男,1977 年生,网络工程师,学士,主要研究方向:IP 网络、ASP.NET WEB 工程、光通信。