

设置系统日志服务器获取从D98xx系列IRDs的日志

目录

[简介](#)

[背景信息](#)

[配置系统日志服务器](#)

[配置IRD \(D9854/D9858/D9859\)发送日志对Syslog观察员](#)

[导出对CSV文件的存储的消息](#)

[删除以前消息](#)

简介

本文描述如何设置系统日志服务器获取从D98xx系列集成接收方/编码器(IRDs)的日志。

背景信息

D9854软件版本4.0、D9858 & D9824和D9859支持RFC-3164兼容系统消息任何版本。客户能当前捕获消息用存储设备和检索的一个系统日志服务器。另外，此步骤可能也与新的D9800网络传输接收方一起使用。

Syslog观察员是Windows机器的支持的自由系统日志服务器。对于Linux机器，从http是可得到的支持的系统日志服务器是Syslog NG [:/www.balabit.com/network-security/syslog-ng/opensource-logging-system](http://www.balabit.com/network-security/syslog-ng/opensource-logging-system)

此条款仅处理在Windows机器的安装。

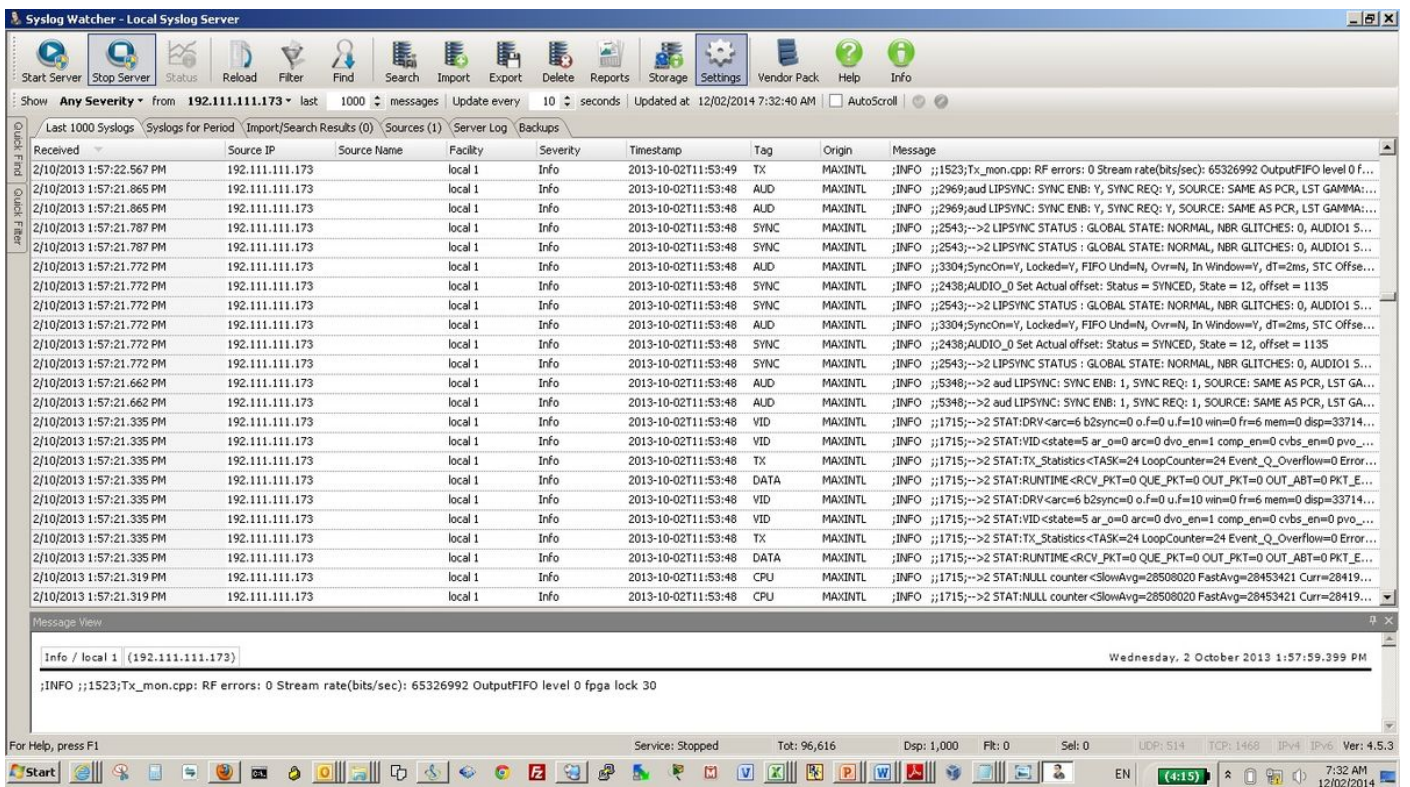
配置系统日志服务器

下载Syslog观察员从

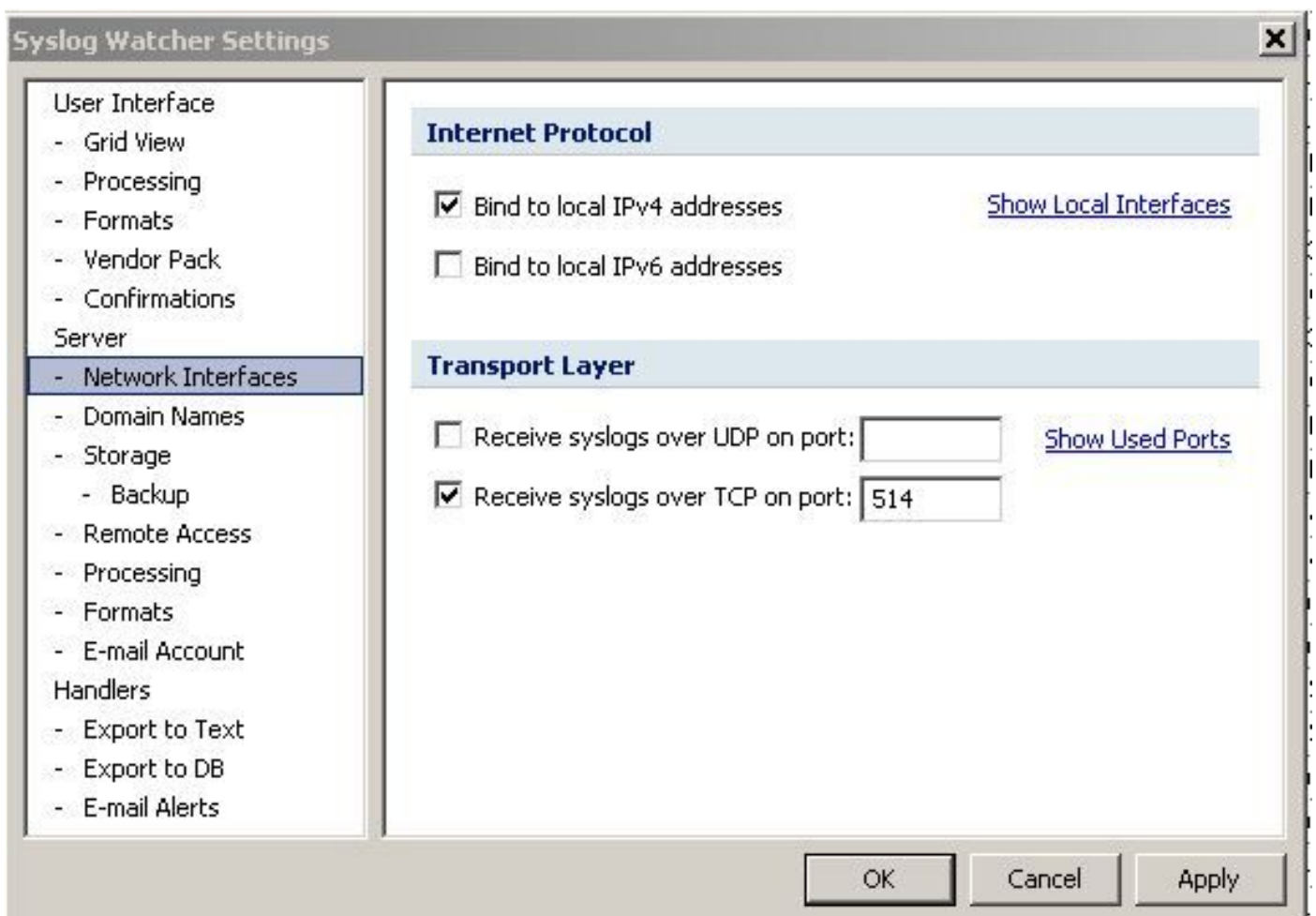
[http : /www.snmpsoft.com/syslogwatcher/syslog-server.html](http://www.snmpsoft.com/syslogwatcher/syslog-server.html)

并且请安装它在您的windows计算机。

开始Syslog观察员并且选择GUI的操作模式和管理本地系统日志服务器，此处显示的图像出现：

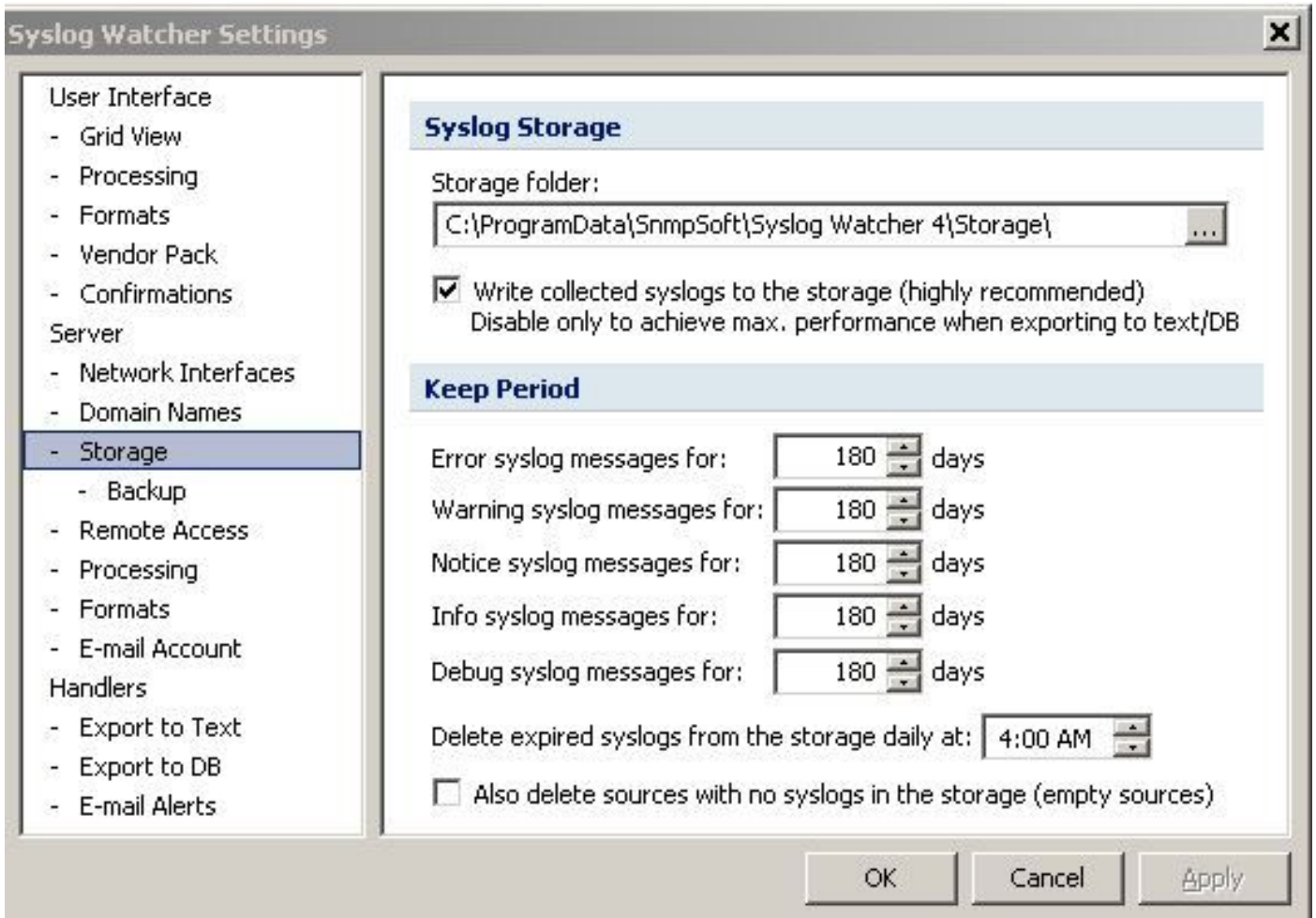


单击在**设置**(突出显示用上述图片)在工具栏，此处显示的图像出现：



选择**网络接口**。检查在**UDP**的方框接收Syslog在端口并且输入端口编号。相同端口端口号在设备需要配置从Syslog观察员需要接收日志。

如镜像所显示，现在请选择存储设备在Syslog观察员设置下，：

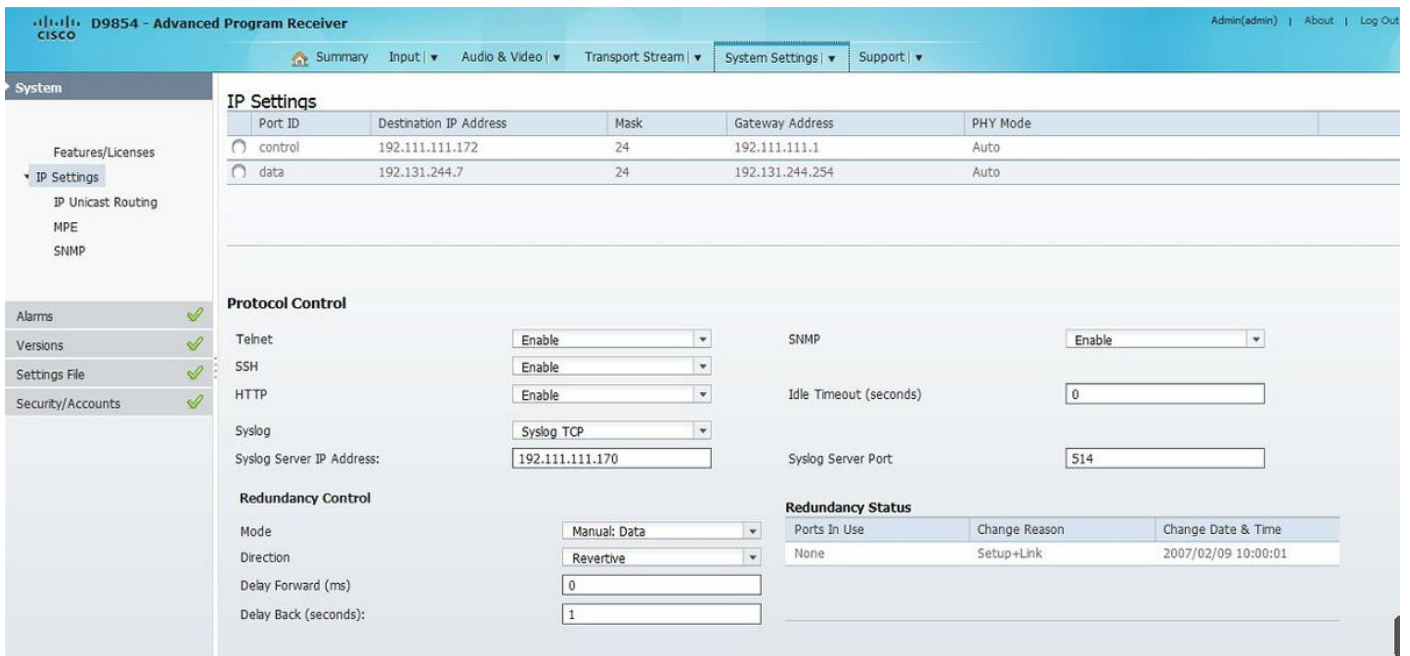


指定存储的消息一个文件夹位置，检查方框Write收集的Syslog到存储设备。

指定几天数量在存储设备能将保留的每种消息类型的。

配置IRD (D9854/D9858/D9859)发送日志对Syslog观察员

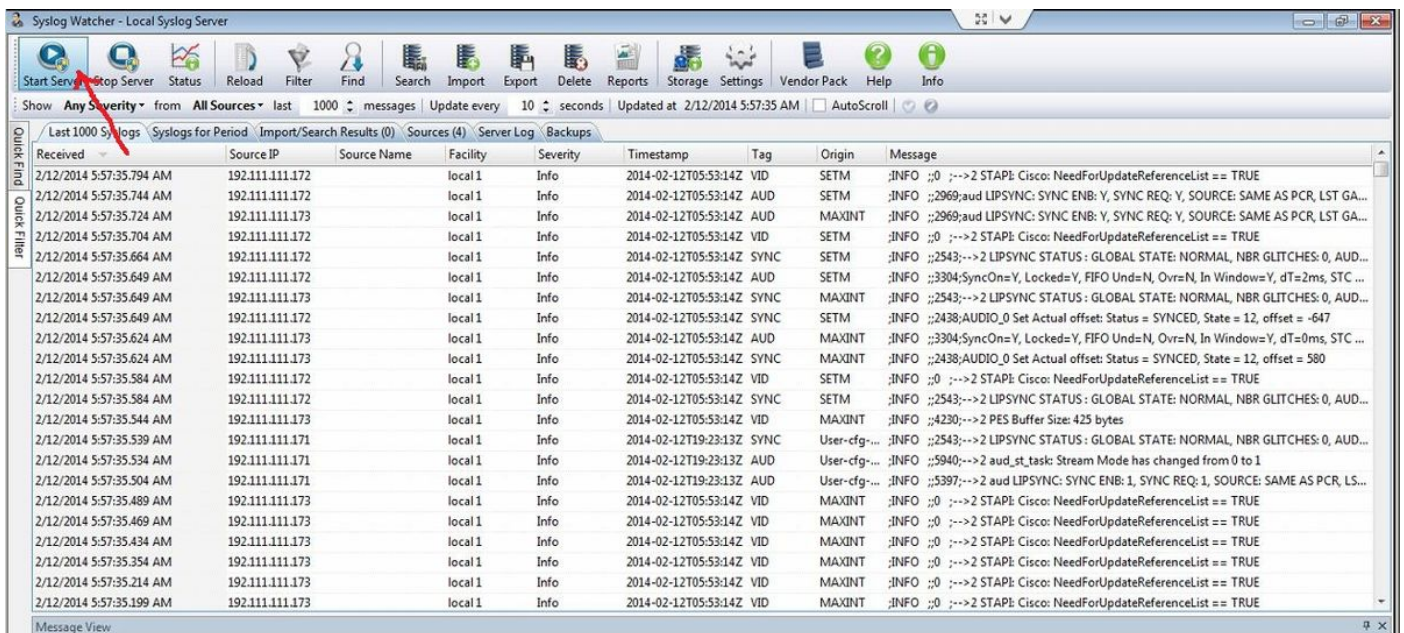
在IRD GUI，请选择从工具栏的系统设置IP设置。此处显示的图像出现：



在Settings页的IP的协议控制部分，请配置这些：

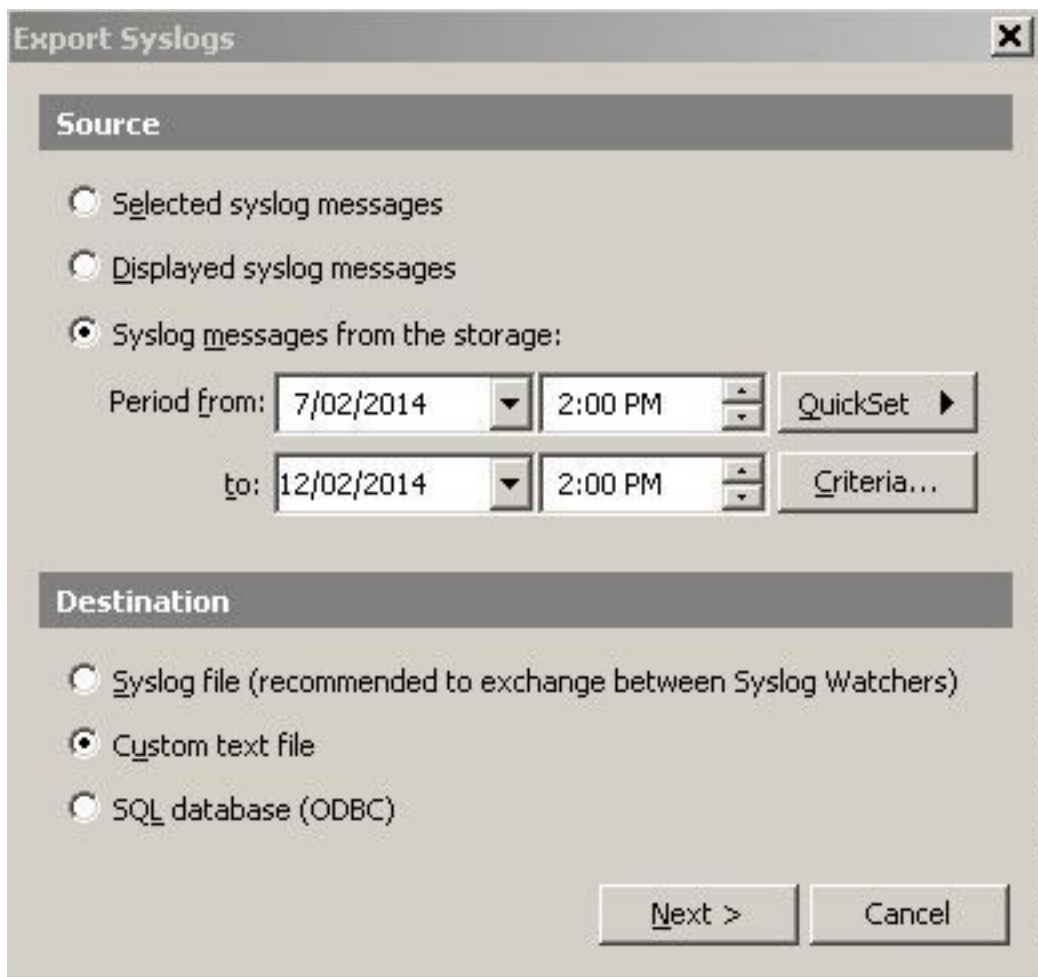
- Syslog-选择Syslog TCP或Syslog UDP如所需求。
- 系统日志服务器IP地址回车Syslog观察员安装计算机的IP地址。
- 系统日志服务器端口回车端口编号。这应该匹配在Syslog观察员设置输入的端口号。

如镜像所显示，在Syslog观察员GUI下，请通过选择启动服务器开始服务，：



导出对CSV文件的存储的消息

在Syslog观察员GUI，请单击在Export按钮在工具栏，如镜像所显示，启动屏幕。



您能选择导出消息在一个特定期限利益或导出仅一特定的选择。在上述屏幕中，它选择导出在期限，发生的消息。

在目的地下，请选择自定义文本文件并且其次单击。

Export to Text File [X]

Destination Files

Export root folder: [Explore Folder](#)

Subfolder: \ Filename: Tag ▶

Create next file when the size is more than: KBytes

Processing Options

Trim large syslog messages to: characters

Preprocess message for:

Line ending: Encoding:

File Format

File header: Tag ▶
Lines: 0

Message conversion template: Tag ▶
Lines: 1

File footer: Tag ▶
Lines: 0

选择目的地文件夹，添加子文件夹并且给予与.csv分机的一个文件名。如果子文件夹不存在，创建。

单击在出口。

删除以前消息

在Syslog观察员GUI，请单击在工具栏的**删除**，如镜像所显示，启动屏幕，：



定义您在**删除**希望删除消息和单击的期限。您也许，使用树篱的按钮迅速选择预定义的期限类似为时一天或一周等。