目录

[第一章API 3](#_Toc384391858)

[1.1 NSSetUncaughtExceptionHandler(NSUncaughtExceptionHandler\*) 3](#_Toc384391859)

[1.2 NSUncaughtExceptionHandler(NSException\*) 3](#_Toc384391860)

[1.3 NSException 3](#_Toc384391861)

[第二章 Sample Code for API 3](#_Toc384391862)

[2.1 project 3](#_Toc384391865)

[2.2 Throw exception program 4](#_Toc384391866)

[2.3 Verify the exception handler 4](#_Toc384391867)

[2.3.1 监控内容 4](#_Toc384391868)

[2.4 子菜单-表格视图 4](#_Toc384391869)

[2.5 子菜单-柱状视图 5](#_Toc384391870)

[2.6 子菜单-曲线视图 5](#_Toc384391871)

[2.7 后台通信协议 6](#_Toc384391872)

[第三章 高级监控 8](#_Toc384391873)

[1. 左侧子菜单的内容 8](#_Toc384391879)

[2. 服务器选择 8](#_Toc384391880)

[3. 业务指标监控 8](#_Toc384391881)

[4. 解析类型监控 9](#_Toc384391882)

[5. 应答类型监控 9](#_Toc384391883)

[第四章 安全事件分析 10](#_Toc384391884)

[1. 左侧子菜单的内容 10](#_Toc384391886)

[2. 流量分析 11](#_Toc384391887)

[1. 子菜单 11](#_Toc384391888)

[2. 查询类型TOP排名 11](#_Toc384391889)

[3. 应答类型TOP排名 13](#_Toc384391890)

[4. 成功率异常分析 15](#_Toc384391891)

[5. 延迟异常分析 15](#_Toc384391892)

[6. 省外用户访问分析 16](#_Toc384391893)

[7. 用户流量异常分析 16](#_Toc384391894)

[8. 域名流量异常分析 16](#_Toc384391895)

[9. 递归流量异常分析 17](#_Toc384391896)

[10. 缓存投毒分析 17](#_Toc384391897)

[第五章 DNS流量分析 19](#_Toc384391898)

[1. 左侧子菜单的内容 19](#_Toc384391900)

[2. 活跃用户 19](#_Toc384391901)

[3. 注册域名 20](#_Toc384391902)

[4. 首位解析地址 21](#_Toc384391903)

[5. 溯源 21](#_Toc384391904)

[第六章 告警 22](#_Toc384391905)

[2.1 左侧子菜单的内容 22](#_Toc384391907)

[2.2 最近告警 22](#_Toc384391908)

[2.3 历史告警 23](#_Toc384391909)

[2.4 告警统计 24](#_Toc384391910)

[第七章 报表 24](#_Toc384391911)

[3.1 左侧子菜单的内容 24](#_Toc384391913)

[第八章 系统工具 24](#_Toc384391914)

[4.1 左侧子菜单的内容 24](#_Toc384391916)

[4.2 用户管理 25](#_Toc384391917)

[1. 子菜单 25](#_Toc384391918)

[2. 新用户注册 25](#_Toc384391919)

[3. 口令修改 25](#_Toc384391920)

[4. 权限修改 25](#_Toc384391921)

[5. 用户操作记录 25](#_Toc384391922)

[4.3 系统配置 26](#_Toc384391923)

[1. 基本配置项 26](#_Toc384391924)

[2. 告警配置项 26](#_Toc384391925)

[第九章 帮助 27](#_Toc384391926)

[附录 27](#_Toc384391927)

[协议规范 27](#_Toc384391928)

[数据库 30](#_Toc384391929)

# 第一章API

## NSSetUncaughtExceptionHandler(NSUncaughtExceptionHandler\*)

注册一个异常处理函数，当有异常没有被捕获的时候，这个处理函数就会被调用。

## NSUncaughtExceptionHandler(NSException\*)

异常处理回调函数

## NSException

使用socket和后台系统通信，采用特定的协议，协议格式见附录协议部分。前台系统需要存储系统配置、用户配置等信息，详细的数据库表见附录的数据库部分。

是一个类，可以创建exception和查询exception的内容。

创建API

exceptionWithName:reason:userInfo:

raise:format:

raise:format:arguments:

initWithName:reason:userInfo:

raise:

查询API：

name

reason

userInfo

callStackReturnAddresses

callStackSymbols

# 第二章 Sample Code for API



## project

* + 服务器选择

1. asdf
   * 表格视图
   * 柱状视图
   * 曲线视图

## Throw exception program

在右侧的显示区显示所有的DNS服务器信息，以表格的形式展示，如下所示。

表2-1 服务器列表

|  |  |  |  |
| --- | --- | --- | --- |
| 选择 | IP地址 | 机器名 | 备注 |
| 勾选框 | 211.15.87.4 | Beijingdns1 | 主DNS服务器 |
| 勾选框 | 211.15.85.5 | Beijingdns2 | 备用DNS服务器 |

读取数据库中的DNS服务器的配置，第一列使用勾选框为用户提供选择显示的服务器。具体的数据库表结构请看附件的配置表汇总。

## Verify the exception handler

## 监控内容

表2-2 监控信息

|  |  |  |
| --- | --- | --- |
| 指标 | 类型 | 例子 |
| QPS | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| PPS | 浮点数，精度到小数点2位 | 104,534.23次/秒 |
| 系统解析成功率 | 百分比，精度到小数点2位 | 99.23% |
| 用户解析成功率 | 百分比，精度到小数点2位 | 99.53% |
| 平均延迟 | 浮点数，精度到小数点2位 | 30.23毫秒 |
| 缓存利用率 | 百分比，精度到小数点2位 | 67.32% |

如上所示为监控信息内容，第一列是5个监控指标，第二列是指标的数值类型，第三列是显示的范例。

还包括了上面指标同类型的历史基线值。

## 子菜单-表格视图

在右侧的显示区以表格的形式展示基本监控信息。表格的信息每5秒刷新一次。形式如下：

表2-3 QPS表格视图

|  |  |  |
| --- | --- | --- |
| 服务器 | QPS值 | 历史基线 |
| 211.15.67.34 | 85,312.23次/秒 | 82,313.21次/秒 |
| 211.15.67.31 | 12,311.45次/秒 | 15,245.14次/秒 |

表2-4 系统解析成功率表格视图

|  |  |  |
| --- | --- | --- |
| 服务器 | QPS值 | 历史基线 |
| 211.15.67.34 | 99.12% | 99.72% |
| 211.15.67.31 | 98.22% | 98.12% |

字体颜色选择：

如果数值 > 基线值 \* 115% 字体为红色；

如果数值 < 基线值 \* 85% 字体为黄色；

否则字体为黑色

这里有一些例外：对于用户解析成功率和系统解析成功率不需要设置红色字体。

## 子菜单-柱状视图

在右侧的显示区以柱状图的形式展示基本监控信息。信息每5秒刷新一次。形式如下：

图2-1 QPS柱状图示意

如图所示，每个服务器用一个柱状图的柱表示，每个指标用一个柱状图表示。

柱的颜色：

如果数值 > 基线 \* 115% 柱为红色

如果数值 < 基线 \* 85% 柱为黄色

否则为蓝色

这里有一些例外：对于用户解析成功率和系统解析成功率不需要设置红色。

## 子菜单-曲线视图

在右侧的显示区以曲线图的形式展示基本监控信息。信息每5秒刷新一次。形式如下：

图2-2 曲线示意图

如图所示，每个曲线表示一个服务器的历史曲线。不同的server的曲线用不同的颜色。每个曲线动态变化，每5秒刷新一次。在显示区上面加一个下拉框-基线选择，分别是各个服务器和不显示基线。当用户选择某个服务器的基线的时候，在曲线图上画基线的上线和下线。分别用红色和黄色表示。如果选择不显示基线则不画基线曲线。

曲线时间段的选择功能：为用户提供四种时间类型：小时、日、月、年。在选定时间类型后，选择具体的时间。比如选择类型为日，具体时间为2013-12-25 00:00:00。

## 后台通信协议

* 后台通信协议关键词

cmd:serverlist – 查询服务器列表

server:serverip – 查询的服务器IP地址（可选值:serverlist中的IP；ALL：表示全部服务器）

cmd:basic – 查询基本监控信息

timetype:type – 时间的类型(可选值: year, month, day, hour)

time: 2013-12-25 00:00:00

* 获取服务器列表

query packet:

cmd:serverlist\n\n

response packet:

192.168.1.1\n192.168.1.2\nbeijingdnsserver1\n递归服务器1\n192.168.1.1\n192.168.1.2\nbeijingdnsserver2\n缓存服务器2\n

\*说明：query packet中"cmd:serverlist"表示查询类型是serverlist。response packet返回以\n分割的服务器IP地址，最后以一个空行\n标识结束response packet。

* 获取basic监控信息

query packet:

cmd:basic\nserver:192.168.1.1\nlasttime:300\n\n

response packet:

23.97\n27.42\n97.37\n95.51\n33.00\n87.26\n\n

\*说明：query packet中"cmd:basic"表示查询类型是basic，"server:192.168.1.1"表示查询服务器192.168.1.1的basic信息， "lasttime:300"表示查询最近300秒（5分钟）的basic信息。web界面的基本监控部分每次刷新都发送这个query，即可以获取最近的basic信息，其中"server:192.168.1.1"可以改为"server:all"表示查询所有服务器basic的汇总值，response packet中的用\n分割统计值，最后以空行\n标识response packet结束。统计值的意义为：QPS\nPPS\n系统解析成功率\n用户解析成功率\n平均延迟\n缓存利用率\n

* 获取basic监控信息基线

query packet:

cmd:basic\nserver:192.168.1.1\nlasttime:300\nbaseline:yes\n\n

response packet:

23.97\n27.42\n97.37\n95.51\n33.00\n87.26\n\n

\*说明：在query packet增加"baseline:yes"表示查询基线,response packet的格式和上面的格式一致。

* 获取basic监控信息曲线视图

query packet:

cmd:basic\nserver:192.168.1.1\nstarttime:1314533556\nendtime:1314533856\n\n

response packet:

23.97\n27.42\n97.37\n95.51\n33.00\n87.26\n\n

\*说明：query packet中用"starttime:1314533556\nendtime:1314533856\n"代替了"lasttime:300\n",这样表示查询在startttime和endtime之间的统计值.response packet格式不变，web界面在绘制一段时间的曲线时,需要将这个时间段分割成n段,然后循环发送n次请求,这样得到了各个小时间段的信息。

例如需要绘制8:00 - 9:00的曲线,页面时间轴定义了10个点.

这样我们得到步长为step = 3600 / 10 = 360秒.用如下为伪代码实现获取一段时间的统计值

for (i = 0; i < 10; i++)

{

starttime = time(8:00) + i \* step; //获取时间点，每次循环starttime增加一个步长

endtime = starttime + step - 1;

basicinfo = query\_for\_basic(starttime, endtime);//查询starttime和endtime之间的统计量

print\_basicinfo\_point(bascinfo);//画点

}

# 第三章 高级监控



## 左侧子菜单的内容

* 服务器选择
* 业务指标监控
* 解析类型监控
* 解析应答监控

## 服务器选择

和基本监控相同

## 业务指标监控

展示形式和基本监控相同，要有表格、柱状图、曲线图。视图选择在左侧菜单的二级子菜单。

数据如下表，通过socket获取。

表3-1 业务指标

|  |  |  |
| --- | --- | --- |
| 指标 | 类型 | 例子 |
| 递归查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 递归查询比例 | 百分比，精度到小数点2位 | 68.23% |
| 缓存查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 缓存查询比例 | 百分比，精度到小数点2位 | 45.53% |
| 应答平均延迟 | 浮点数，精度到小数点2位 | 30.23毫秒 |
| 递归平均延迟 | 百分比，精度到小数点2位 | 300.23毫秒 |

* 后台通信协议关键词

cmd:apply – 查询业务指标

* 后台通信协议

query packet:

cmd:apply\nserver:192.168.1.1\nlasttime:300\n\n

response packet:

7.07\n24.79\n0.00\n249.00\n22.20\n77.80\n\n

\*说明："cmd:apply"表示查询业务指标，其他格式和基本监控相同response packet的各个段的意义如下：递归查询\n缓存查询\n应答平均延迟\n递归平均延迟\n递归查询比例\n缓存查询比例\n\n

## 解析类型监控

展示形式和业务指标相同，指标如下表：

表3-2 解析类型指标

|  |  |  |
| --- | --- | --- |
| 指标 | 类型 | 例子 |
| A查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| A查询比例 | 百分比，精度到小数点2位 | 68.23% |
| MX查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| MX查询比例 | 百分比，精度到小数点2位 | 68.23% |
| CNAME查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| CNAME查询比例 | 百分比，精度到小数点2位 | 68.23% |
| PTR查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| PTR查询比例 | 百分比，精度到小数点2位 | 68.23% |
| TXT查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| TXT查询比例 | 百分比，精度到小数点2位 | 68.23% |
| 其他查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 其他查询比例 | 百分比，精度到小数点2位 | 68.23% |

* 后台通信协议关键词

cmd:qtype – 查询解析类型

* 后台通信协议

query packet:

cmd:qtype\nserver:192.168.1.1\nlasttime:300\n\n

response packet:

4.79\n0.14\n1.58\n0.30\n1.28n10.39\n25.92\n0.76\n8.55\n1.62\n6.93\n56.22\n\n

\*说明:"cmd:qtype"表示查询解析类型，其他格式相同response packet的各个段的意义如下：

A查询数\nMX查询数\nCNAME查询数\nPTR查询数\nTXT查询数\n其他查询数\nA查询比例\nMX查询比例\nCNAME查询比例\nPTR查询比例\nTXT查询比例\n其他查询比例\n\n

## 应答类型监控

展示形式和业务指标相同，指标如下表：

表3-2 解析类型指标

|  |  |  |
| --- | --- | --- |
| 指标 | 类型 | 例子 |
| 用户解析成功数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 系统解析成功数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 错误域名数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 错误域名比例 | 百分比，精度到小数点2位 | 68.23% |
| 系统错误数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 系统错误比例 | 百分比，精度到小数点2位 | 68.23% |
| 格式错误数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| 格式错误比例 | 百分比，精度到小数点2位 | 68.23% |
| DNSSEC查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| DNSSEC查询比例 | 百分比，精度到小数点2位 | 68.23% |
| EDNS0查询数 | 浮点数，精度到小数点2位 | 80,032.33次/秒 |
| EDNS0查询比例 | 百分比，精度到小数点2位 | 68.23% |

* 后台通信协议关键词

cmd:rcode – 查询应答类型

* 后台通信协议

query packet:

cmd:rcode\nserver:192.168.1.1\nlasttime:300\n\n

response packet:

4.79\n0.14\n1.58\n0.30\n1.28n10.39\n25.92\n0.76\n8.55\n1.62\n6.93\n56.22\n\n

\*说明:"cmd:rcode"表示查询应答类型，其他格式相同response packet的各个段的意义如下：

用户解析成功数\n系统解析成功数\n错误域名数\n错误域名比例\n系统错误数\n系统错误比例\n格式错误数\n格式错误比例\nDNSSEC查询数\nDNSSEC查询比例\nEDNS0查询数\nEDNS0查询比例\n\n

高级监控的基线查询和基本监控的基线查询类似，在query packet中加入"baseline:yes\n"表示查询基线

曲线的查询也要通过循环查询各个点的信息

# 第四章 安全事件分析



## 左侧子菜单的内容

* 服务器选择
* 流量分析
* 成功率异常分析
* 延迟异常分析
* 省外用户访问分析
* 用户流量异常分析
* 域名流量异常分析
* 域流量异常分析
* 递归流量异常分析
* 缓存投毒分析

## 流量分析

## 子菜单

* + 按查询类型TOP排名
  + 按应答类型TOP排名

## 查询类型TOP排名

通过socket得到查询类型TOP排名，参见附录中协议部分的说明。得到数据后使用表格形式展示。格式如下表所示。

表4-1 TOP查询类型排名

|  |  |  |
| --- | --- | --- |
| 域名 | A记录查询比例 | A记录查询速率 |
| [www.xxxx.com](http://www.xxxx.com) | 45.11% | 56,743.32次/秒 |
| [www.yyyy.com](http://www.yyyy.com) | 12.10% | 13,412.12次/秒 |

在顶部用一个下拉框选择查类型：包括A，MX，CNAME，PTR。类型选择的右侧有一个时间选择，可以指定某天，某天的时间段的TOP（时间段以小时为基本单位）。

* 后台通信协议关键词：

timetype:type – 时间的类型(可选值: year, month, day, hour, min)

time:utc – 时间点(根据用户选定的时间类型和值，将其转化为UTC时间，例如

用户选择2003-04-04，时间类型是timetype:day。这样选择2003-04-04 00:00:00 – 2003-04-04 23:59:59中的任意一秒作为时间点，这样后台可以余数运算确定具体日期)

recordstart:no – (查询TOP记录的起始位置。可选值:>=0的整数)

recordnumber:number – (从recordstart开始的查询TOP记录的个数。可选值>0的整数)

domainlevel:level – 域的级别(可选值：0：域名；> 0 表示分级的域)

cmd:topqtypea - 查询A类型

sortedby:qtypearate - 按A记录查询比例排序

sortedby:qtypeaps - 按A记录查询量排序

cmd:topqtypemx - 查询MX类型

sortedby:qtypemxrate - 按MX记录查询比例排序

sortedby:qtypemxps - 按MX记录查询量排序

cmd:topqtypecname - 查询CNAME类型

sortedby:qtypecnamerate - 按CNAME记录查询比例排序

sortedby:qtypecnameps - 按CNAME记录查询量排序

cmd:topqtypeptr - 查询PTR类型

sortedby:qtypeptrrate - 按PTR记录查询比例排序

sortedby:qtypeptrps - 按PTR记录查询量排序

cmd:topqtypetxt - 查询TXT类型

sortedby:qtypetxtrate - 按TXT记录查询比例排序

sortedby:qtypetxtps - 按TXT记录查询量排序

cmd:topqtypeother - 查询其他类型

sortedby:qtypeotherrate - 按其他记录查询比例排序

sortedby:qtypeotherps - 按其他记录查询量排序

* 后台通信协议
  + 1. 查询类型A

query packet:

cmd:topqtypea\nserver:192.168.1.1\nsortedby:qtypearate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:0\n\n

response packet:

www.sina.com.cn,26.40,26.40,27.39\nwww.baidu.com.cn,18.30,18.30,20.59\n\n

\*说明：

query packet中"cmd:topqtypea"表示查询查询类型A的TOP，"sortedby:qtypearate"表示按照A记录查询比例排序，可以选择”sortedby:qtypeaps”表示按照A记录查询量排序，"starttime:1314533556\nendtime:1314533856"表示在starttime和endtime之间累计，"domainlevel:0"表示查询域名，如果"domainlevel:1"表示查询一级域名，"domainlevel:2"表示查询二级域名，response packet:用\n分割记录。一个记录"www.sina.com.cn,26.40,26.40,27.39\n"中www.sina.com.cn是域名字段，然后是"A查询比例,A查询量,"用逗号分割。

* + 1. 查询类型MX

query packet:

cmd:topqtypemx\nserver:192.168.1.1\nsortedby:qtypemxrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:0\n\n

response packet:

www.sina.com.cn,26.40,26.40,27.39\nwww.baidu.com.cn,18.30,18.30,20.59\n\n

* + 1. 查询类型CNAME

query packet:

cmd:topqtypecname\nserver:192.168.1.1\nsortedby:qtypecnamerate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:0\n\n

response packet:

www.sina.com.cn,26.40,26.40,27.39\nwww.baidu.com.cn,18.30,18.30,20.59\n\n

* + 1. 查询类型PTR

query packet:

cmd:topqtypeptr\nserver:192.168.1.1\nsortedby:qtypeptrrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:0\n\n

response packet:

www.sina.com.cn,26.40,26.40,27.39\nwww.baidu.com.cn,18.30,18.30,20.59\n\n

* + 1. 查询类型TXT

query packet:

cmd:topqtypetxt\nserver:192.168.1.1\nsortedby:qtypetxtrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:0\n\n

response packet:

www.sina.com.cn,26.40,26.40,27.39\nwww.baidu.com.cn,18.30,18.30,20.59\n\n

* + 1. 其他查询类型

query packet:

cmd:topqtypeother\nserver:192.168.1.1\nsortedby:qtypeotherrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:0\n\n

response packet:

www.sina.com.cn,26.40,27.39\nwww.baidu.com.cn,18.30,20.59\n\n

## 应答类型TOP排名

用表格形式展示TOP。表格形式如下。

表4-2 TOP应答类型排名

|  |  |  |
| --- | --- | --- |
| 域名 | 无应答比例 | 无应答次速率 |
| [www.xxxx.com](http://www.xxxx.com) | 45.11% | 56,743.32次/秒 |
| [www.yyyy.com](http://www.yyyy.com) | 12.10% | 13,412.12次/秒 |

在顶部用一个下拉框选择应答类型：包括解析正确，错误域名，服务失败，无应答，无应答递归，无应答授权服务器。

* 后台通信协议关键词：

cmd:topnoerror - 查询解析正确排名

sortedby:noerrorrate – 按解析正确比例排序

sortedby:noerrorps – 按解析正确量排序

cmd:topnxdomain – 查询错误域名排名

sortedby:nxdomainrate – 按错误域名查询比例排序

sortedby:nxdomainps – 按错误域名查询量排序

cmd:servfail – 查询服务失败排名

sortedby: servfailrate – 按服务失败查询比例排序

sortedby: servfailps – 按服务失败查询量排序

cmd:timeout – 查询无应答排名

sortedby: timeoutrate – 按无应答比例排序

sortedby: timeoutps – 按无应答量排序

cmd:timeoutrecur – 查询无应答递归排名

sortedby: timeoutrecurrate – 按无应答递归比例排序

sortedby: timeoutrecurps – 按无应答递归量排序

cmd:timeoutauth – 查询无应答授权服务器排名

sortedby: timeouauthrate – 按授权服务器无应答比例排序

sortedby: timeoutauthps – 按授权服务器无应答量排序

* 1. 解析正确

query packet:

cmd:topnoerror\nserver:192.168.1.1\nsortedby:noerrorrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,18.30,20.59\n\n

* 1. 错误域名

query packet:

cmd:topnxdomain\nserver:192.168.1.1\nsortedby:nxdomainrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,18.30,20.59\n\n

* 1. 服务失败

query packet:

cmd:topservfail\nserver:192.168.1.1\nsortedby:servfailrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,18.30,20.59\n\n

* 1. 无应答

query packet:

cmd:toptimeout\nserver:192.168.1.1\nsortedby:timeoutrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,18.30,20.59\n\n

* 1. 无应答递归

query packet:

cmd:toptimeoutrecur\nserver:192.168.1.1\nsortedby:timeoutrecurrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,18.30,20.59\n\n

* 1. 无应答授权服务器

query packet:

cmd:toptimeoutauth\nserver:192.168.1.1\nsortedby:timeoutauthrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,211.15.64.23,26.40,27.39\nbaidu.com.cn,211.15.62.23,18.30,20.59,\n\n

无应答授权服务器的格式和其他不同，如下所示。

表4-3 TOP应答类型排名

|  |  |  |  |
| --- | --- | --- | --- |
| 授权服务器域 | 授权服务器IP | 无应答比例 | 无应答次速率 |
| com.cn | 211.15.64.23 | 45.11% | 56,743.32次/秒 |
| xxx.org.net | 211.15.62.23 | 12.10% | 13,412.12次/秒 |

## 成功率异常分析

用表格形式展示。表格如下：

表4-4 TOP异常域名排名

|  |  |  |
| --- | --- | --- |
| 异常域名 | 解析失败比例 | 解析失败速率 |
| www.xxx.com | 45.11% | 56,743.32次/秒 |
| www.xxx.org | 12.10% | 13,412.12次/秒 |

* 后台通信协议关键词：

cmd:fail – 查询解析失败排名

sortedby:failrate – 按照解析失败比例排序

sortedby:failps – 按照解析失败量排序

query packet:

cmd:fail\nserver:192.168.1.1\nsortedby:failrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,18.30,20.59\n\n

## 延迟异常分析

用表格形式展示。表格如下：

表4-5 TOP延迟异常域名排名

|  |  |  |  |
| --- | --- | --- | --- |
| 异常域名 | 查询比例 | 查询速率 | 平均延迟 |
| www.xxx.com | 45.11% | 56,743.32次/秒 | 2000毫秒 |
| www.xxx.org | 12.10% | 13,412.12次/秒 | 2100毫秒 |

* 后台通信协议关键词：

cmd:delay – 查询延迟排序

sortedby:qrate – 按照查询比例排序

sortedby:qps – 按照查询两排序

sortedby:delay – 按照平均延迟排序

query packet:

cmd:delay\nserver:192.168.1.1\nsortedby:qrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,27.39,26.40,3452.23\nbaidu.com.cn,20.59,8.30,1123.12\n\n

## 省外用户访问分析

用表格形式展示。表格如下：

表4-6 TOP省外用户排名

|  |  |  |
| --- | --- | --- |
| 省外用户IP | 查询比例 | 查询速率 |
| 211.123.23.45 | 45.11% | 56,743.32次/秒 |
| 210.13.24.11 | 12.10% | 13,412.12次/秒 |

* 后台通信协议关键词：

cmd:outerclient – 查询省外用户排序

query packet:

cmd:outerclient\nserver:192.168.1.1\nsortedby:qrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

211.123.23.45,26.40,27.39\n210.13.24.11,8.30,20.59\n\n

## 用户流量异常分析

用表格形式展示。表格如下：

表4-8 TOP用户查询排名

|  |  |  |
| --- | --- | --- |
| 用户IP | 查询比例 | 查询速率 |
| 211.123.23.45 | 45.11% | 56,743.32次/秒 |
| 210.13.24.11 | 12.10% | 13,412.12次/秒 |

* 后台通信协议关键词：

cmd:client – 查询用户排序

query packet:

cmd:client\nserver:192.168.1.1\nsortedby:qrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

211.123.23.45,26.40,27.39\n210.13.24.11,8.30,20.59\n\n

## 域名流量异常分析

用表格形式展示。表格如下：

表4-10 TOP域名查询排名

|  |  |  |
| --- | --- | --- |
| 域名 | 查询比例 | 查询速率 |
| www.xxx.com | 45.11% | 56,743.32次/秒 |
| www.yyy.net | 12.10% | 13,412.12次/秒 |

* 后台通信协议关键词：

cmd:qname – 查询域名排序

query packet:

cmd:qname\nserver:192.168.1.1\nsortedby:qrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,8.30,20.59\n\n

## 递归流量异常分析

用表格形式展示。有一个下拉框选择域的级，最多到3级。表格如下：

表4-14 TOP递归查询排名

|  |  |  |
| --- | --- | --- |
| 域名 | 递归查询比例 | 递归查询速率 |
| xxx.com | 45.11% | 56,743.32次/秒 |
| yyy.net | 12.10% | 13,412.12次/秒 |

* 后台通信协议关键词：

cmd:recur – 查询递归排序

sortedby:recurrate – 按递归比例排序

sortedby:recurps – 按递归查询速率排序

query packet:

cmd:recur\nserver:192.168.1.1\nsortedby:recurrate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26.40,27.39\nbaidu.com.cn,8.30,20.59\n\n

## 缓存投毒分析

用表格形式展示。有一个下拉框选择域的级，最多到3级。表格如下：

表4-16 TOP投毒排名

|  |  |  |
| --- | --- | --- |
| 域名 | 投毒次数 | 递归查询速率 |
| xxx.com | 2,345 | 56,743.32次/秒 |
| yyy.net | 1,234 | 13,412.12次/秒 |

* 后台通信协议关键词：

cmd:hijack – 查询投毒排序

sortedby:hijackps – 按投毒次数排序

query packet:

cmd:hijack\nserver:192.168.1.1\nsortedby:hijackps\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\ndomainlevel:3\n\n

response packet:

sina.com.cn,26,27.39\nbaidu.com.cn,18,20.59\n\n

# 第五章 DNS流量分析



## 左侧子菜单的内容

* 活跃用户
* 注册域名
* 首位解析地址
* 溯源
* 域分析
* 重点域名分析
* 子域分析

## 活跃用户

使用表格展示。在顶部显示活跃用户数。有一个下拉框包含选择了排名的列，分别如下：查询比例，QPS，解析成功率，递归查询率，缓存查询率，缓存命中率。

表5-1 活跃用户

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 用户IP | 查询比例 | QPS | 解析成功率 | 递归查询率 | 缓存查询率 | 缓存命中率 |
| 211.123.23.45 | 45.11% | 743.32次/秒 | 89.12% | 24.21次/秒 | 721.12次/秒 | 56.12% |
| 210.13.24.11 | 12.10% | 412.12次/秒 | 97.11% | 53.12次/秒 | 347.22次/秒 | 23.12% |

* 后台通信协议关键词：

cmd:activeclientnum – 查询活跃用户数

cmd:activeclient – 查询活跃用户

sortedby:qrate – 按照查询比例排序

sortedby:cacheps – 按照缓存查询率排序

sortedby:cacherate – 按照缓存命中率排序

sortedby:qps – 按照qps排序  
sortedby:noerrorrate – 按解析成功率排序

sortedby:recurps – 按递归查询率排序

sortedby:cacheps – 按照缓存查询率排序

sortedby:cacherate – 按照缓存命中率排序

活跃用户数：

query packet:

cmd:activeclientnum\nserver:192.168.1.1\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\n\n

response packet:

3455122\n\n

活跃用户：

query packet:

cmd:activeclient\nserver:192.168.1.1\nsortedby:qps\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\n\n

response packet:

211.123.23.45,45.11,743.32,89.12,24.21,721.12,56.12\n210.13.24.11,12.10,412.12,97.11,53.12,347.22,23.12\n\n

## 注册域名

使用表格展示。在顶部显示注册域名数。有一个下拉框包含选择了排名的列，分别如下：查询比例，QPS，解析成功率，递归查询率，缓存查询率，缓存命中率。

表5-2 注册域名

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 注册域名 | 查询比例 | QPS | 解析成功率 | 递归查询率 | 缓存查询率 | 缓存命中率 |
| www.xxx.com | 45.11% | 743.32次/秒 | 89.12% | 24.21次/秒 | 721.12次/秒 | 56.12% |
| www.yyy.net | 12.10% | 412.12次/秒 | 97.11% | 53.12次/秒 | 347.22次/秒 | 23.12% |

* 后台通信协议关键词：

cmd:registernamenum – 查询注册域名数

cmd:registername – 查询注册域名

sortedby:qps – 按照qps排序

sortedby:noerrorrate – 按解析成功率排序

sortedby:recurps – 按递归查询率排序

sortedby:cacheps – 按照缓存查询率排序

sortedby:cacherate – 按照缓存命中率排序

注册域名数:

query packet:

cmd:registernamenum\n\n

response packet:

4523445\n\n

注册域名:

query packet:

cmd:registername\nsortedby:qps\nrecordstart:100\nrecordnumber:100\n\n

response packet:

www.xxx.com,45.11,743.32,89.12,24.21,721.12,56.12\nwww.yyy.net,12.10,412.12,97.11,53.12,347.22,23.12\n\n

## 首位解析地址

使用表格展示。有一个下拉框包含选择了排名的列，分别如下：比例，应答率，活跃用户数，缓存命中率，平均延迟。

表5-3 首位解析地址

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IP地址 | 域名 | 比例 | 应答率 | 活跃用户数 | 平均延迟 | 缓存命中率 |
| 211.15.12.34 | www.xxx.com | 34.12% | 89.12% | 5812 | 234.12毫秒 | 56.12% |
| 211.16.12.34 | www.yyy.net | 18.12% | 97.11% | 3456 | 347.22毫秒 | 23.12% |

* 后台通信协议关键词：

cmd:firstip – 查询首位解析地址

sortedby:rate – 按比例排序

sortedby:responserate – 按应答率排序

sortedby:activeclient – 按活跃用户数排序

sortedby:cacherate – 按照缓存命中率排序

sortedby:delay – 按照平均延迟排序

query packet:

cmd:firstip\nsortedby:rate\ntimetype:day\ntime:13712312421\nrecordstart:100\nrecordnumber:100\n\n

response packet:

211.15.12.34,www.xxx.com,34.12,89.12,5812,234.12,56.12\n211.16.12.34,www.yyy.net,18.12,97.11,3456,347.22,23.12\n \n

## 溯源

域名输入框、IP输入框、起始时间、结束时间、和确定按钮。当用户输入了所有条件，点击确定按钮后。用socket向后台系统发起请求，后台系统回应结果。

用文本区显示返回的结果。

* 后台通信协议关键词：

cmd:trace – 溯源查询

qname:query-name – 溯源查询的域名(可选值:输入框中的查询域名)

qclient:ip – 溯源查询的客户端(可选之:输入框中的IP地址)

query packet:

cmd:trace\nqname:www.sina.com\nqclient:192.168.4.5\nstarttime:13712312421\nendtime:13712312421\n \n

response packet:

2013-05-06 08:01:11:345563 192.168.4.5 query [www.sina.com](http://www.sina.com) A to 211.45.13.254\n

2013-05-06 08:01:11:567121 211.45.13.254 query [www.sina.com](http://www.sina.com) A to 61.45.14.45\n

2013-05-06 08:01:13:123451 61.45.14.45 response [www.sina.com](http://www.sina.com) A to 211.45.13.254 rcode:zonecut with sina.com ns 56.145.56.13;sina.com ns 56.145.56.11\n

2013-05-06 08:01:13:782455 211.45.13.254 query [www.sina.com](http://www.sina.com) A to 56.145.56.13\n

2013-05-06 08:01:14:134564 56.145.56.13 response [www.siina.com](http://www.siina.com) A to 2111.45.13.254 rcode:noerror with [www.sina.com](http://www.sina.com) A 61.45.67.11;www.sina.com A 61.56.67.12\n

=================================================================\n

2013-05-06 08:01:11:345563 192.168.4.5 query [www.sina.com](http://www.sina.com) A to 211.45.13.254\n

2013-05-06 08:01:11:567121 211.45.13.254 query [www.sina.com](http://www.sina.com) A to 61.45.14.45\n

2013-05-06 08:01:13:123451 61.45.14.45 response [www.sina.com](http://www.sina.com) A to 211.45.13.254 rcode:zonecut with sina.com ns 56.145.56.13;sina.com ns 56.145.56.11\n

2013-05-06 08:01:13:782455 211.45.13.254 query [www.sina.com](http://www.sina.com) A to 56.145.56.13\n

2013-05-06 08:01:14:134564 56.145.56.13 response [www.siina.com](http://www.siina.com) A to 2111.45.13.254 rcode:noerror with [www.sina.com](http://www.sina.com) A 61.45.67.11;www.sina.com A 61.56.67.12\n\n

# 第六章 告警



## 左侧子菜单的内容

* 最近告警
* 历史告警
* 告警统计
* 告警操作

## 最近告警

使用表格显示告警信息，如下所示：

表6-1 最近告警表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | 时间 | 告警名称 | 告警内容 | 告警级别 |
| 1 | 2013/2/24 08:00:30 | 查询流量超过阀值 | 查询流量102,123次/秒，已经超过最大阀值 | 5 |
| 2 | 2013/2/24 18:00:30 | 平均延迟过大 | 平均延迟2001毫秒，超过延迟基线 | 6 |

* 后台通信协议关键词：

cmd:alarm – 告警查询

cmd:alarmanalysis – 告警分析查询

alarmid:告警ID

level: – 告警级别(可选值:0-6 筛选高于level值的告警)

query packet:

cmd:alarm\nserver:192.168.1.1\nlevel:3\nlasttime:3600 \n

response packet

1,2013/04/01 08:09:30,查询流量查过阀值,查询流量102,123次/秒，已经超过最大阀值,5\n2,2013/04/01 08:19:30,查询流量查过阀值,查询流量212,123次/秒，已经超过最大阀值,5\n\n

## 历史告警

有起始时间和结束时间的输入选择。查询后台系统得到告警信息，用下面的表格展示。

表6-1 历史告警表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | 时间 | 告警名称 | 告警内容 | 告警级别 | 分析 |
| 1 | 2013/2/24 08:00:30 | 查询流量超过阀值 | 查询流量102,123次/秒，已经超过最大阀值 | 5 | 分析按钮 |
| 2 | 2013/2/24 18:00:30 | 平均延迟过大 | 平均延迟2001毫秒，超过延迟基线 | 6 | 分析按钮 |

其中分析按钮出发查询后台分析结果，返回后以文本区展示在弹出页面中。

query packet:

cmd:alarm\nserver:192.168.1.1\nlevel:3\nstarttime:13712312421\nendtime:13712312421\n \n

response packet

1,2013/04/01 08:09:30,查询流量查过阀值,查询流量102,123次/秒，已经超过最大阀值,5\n2,2013/04/01 08:19:30,查询流量查过阀值,查询流量212,123次/秒，已经超过最大阀值,5\n\n

分析查询

query packet:

cmd:alarmanalysis\nserver:192.168.1.1\nalaramid:2\n\n

response packet:

txt

## 告警统计

有一个选择框选择告警级别。有起始时间和结束时间选择。然后用曲线显示时间段内高于告警级别的个数。页面程序需要循环读取每个时间点的数据。

* 后台通信协议关键词：

cmd:alarmstatistic – 查询告警统计

query packet:

cmd:alarmstatistic\nserver:192.168.1.1\nlevel:3\nstarttime:13712312421\nendtime:13712312421\n \n

respons packet:

3456\n\n

# 第七章 报表



## 左侧子菜单的内容

* 天报表
* 周报表
* 月报表

有一个日期选择框，选择生成报表的天、周或者月。有一个确认按钮，当点击确认后，显示生成报表的进度条，生成后提示下载框，用户可以下载到本地。

# 第八章 系统工具



## 左侧子菜单的内容

* 用户管理
* 系统配置
* 恢复出厂设置
* 重启
* 导入/导出
* 序列号
* 系统升级
* 系统日志

## 用户管理

## 子菜单

* 新用户注册
* 口令修改
* 权限修改
* 用户操作记录

## 新用户注册

使用普遍的网站用户注册流程和展示样式

## 口令修改

修改用户口令

## 权限修改

用表格列出基本监控、高级监控、安全分析、流量分析、告警、报表、系统工具模块，分别由观察和修改权限。用勾选框确定这个用户是否有这个权限。

## 用户操作记录

如果有查看权限，用表格列出某个用户的操作历史记录。首先用表格展示所有用户的信息。然后一个查看按钮，点击后在下面用表格显示用户操作历史。如下表格：

表8-1 用户表格

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 用户名 | 注册时间 | 最近登陆 | 权限 | 联系方式 | 备注 | 记录 |
| 张三 | 2010/10/12 | 2013/02/24 | 6级 | 13523456781 | 技术部主任 | 查看 |

表8-2 用户操作记录表格

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 用户名 | 时间 | 登录IP | 操作内容 | 退出 |
| 张三 | 2013/02/24 08:33:12 | 211.15.24.45 | 查看基本监控 | 2013/02/24 08:53:12 |

在顶部有一个查看按钮，点击后列出所有用户的操作记录。

## 系统配置

## 基本配置项

表8-3 OPTION配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| Capture-filter | Varchar(256) |
| Capture-eth | Varchar(16) |

表8-4 VIEW配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| View-name | Varchar(16) |

表8-5 match-client配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| Net | Varchar(32) |
| Viewid | int |

表8-6 dns-server-list配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| ip | Varchar(32) |
| Viewid | int |

表8-7 isp-net配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| Net | Varchar(32) |
| Viewid | int |

## 告警配置项

|  |  |
| --- | --- |
| 告警配置 | 说明 |
| 告警级别 | 配置告警过滤级别 |
| 告警管理员 | 配置接收特定告警级别以上的管理员的email,mobile |

# 第九章 帮助

连接到帮助手册。

# 附录

## 协议规范

请求包：

msgid:1234\r\n

cmd:basic-monitor\r\n

data:server=211.15.61.23\r\n

\r\n

应答包：

msgid:1234\r\n

cmd:basic-monitor \r\n

data: qps=80,032.33; 71,052.13\r\n

pps=104,534.23; 114,334.23\r\n

sysok=99.23;99.12\r\n

usrok=99.53;99.11\r\n

delay=30.23;21.22\r\n

cacherate=67.32;64.12\r\n

\r\n

如上所示为协议的样例。协议包含4个部分没个部分以\r\n结束，所有数据为字符串。

* 第一部分msgid：表示一个查询和请求配对，是一个随机数字符串。
* 第二部分cmd：表示这个请求的类型。
* 第三部分data:对应类型数据部分。
* 第四部分\r\n:这个消息包结束标识。

请求类型见下表：

附录协议表1 请求类型

|  |  |  |
| --- | --- | --- |
| 类型 | Data部分 | 说明 |
| Basic-monitor | 请求:server=211.15.61.23\r\n  \*表示需要211.15.61.23的基本信息，如果没有设置server则服务端返回一个汇总的结果 | 基本监控 |
| 应答：  qps=80,032.33; 71,052.13\r\n  pps=104,534.23;114,334.23\r\n  sysok=99.23;99.12\r\n  usrok=99.53;99.11\r\n  delay=30.23;21.22\r\n  cacherate=67.32;64.12\r\n  \*分别表示各个指标的数值。  关键字说明：  Sysok:系统解析成功率  Usrok:用户解析成功率  Delay:平均延迟  Cacherate:缓存命中率  分号分割了实时数值和基线数值。 |
| Advanced-monittor-application | 请求:server=211.15.61.23\r\n  \*和基本监控相同 | 高级监控业务 |
| 应答:格式和基本监空相同。  \*关键字说明：  recurion:递归查询数  recurionrate:递归查询比例  cache:缓存查询数  cacherate:缓存查询比例  cachehit:缓存命中率  querydelay:缓存平均延迟  recursiondelay:递归平均延迟 |
| Advanced-monitor-qtype | 请求格式基本监控相同  应答关键字：  A:a查询数  Arate:a查询比例  Mx：mx查询数  Mxrate：mx查询比例  Cname：cname查询数  Cnamerate:cname查询比例  Txt:txt查询数  Txtrate:txt查询比例  Ptr：ptr查询数  Ptrrate:ptr查询比例  Other:其他查询数  Otherrate:其他查询比例 | 高级监控查询类型 |
| Advanced-monitor-response | 关键字：  Userok:用户解析成功数  Sysok:系统解析成功数 |  |
| Top-type | 请求：  Data:  Type=a\r\n  Byfield=rate\r\n  Timestart=122412341\r\n  Timeend=134335355\r\n  \*type表示需要的类型a、mx、cname、ptr、txt、other。  \*byfield表示按照排序的字段rate、number  \*timestart和timeend是time()的值，time since the Epoch (00:00:00 UTC, January 1, 1970), measured in seconds.  表示取这段时间之间的TOP  应答:  Data:  [www.xxx.com](http://www.xxx.com) 1234.12 32.12%\r\n  [www.yyy.net](http://www.yyy.net) 1234.11 12.24%\r\n |  |
| Top-response | 请求和应答格式和top-type相同  \*response=timeout  表示要TOP的应答类型  \*timeout、nxdomain、formaterror、servfail、timeoutauthority、timeoutrecursion |  |
| Top-delay | 请求:  Byfield=rate\r\n  \*或者qps、delay |  |
| Top-outer-user | 请求:  Data:  Byfield=rate\r\n  \*或者qps |  |
| Top-client | 和上面一样 |  |
| Top-active-user | 请求:  Byfield=rate或者qps、okrate、rps、cps、cacherate |  |
| Top-registed-name | 和上面一样 |  |
| Top-first-ip | 请求:  Byfield:rate、responserate、activenumber、delay、cacherate |  |
| Top-domain | 请求  Data:  \*Level=1、2、3  其他和上面一样 |  |
| Top-vipname | 和上面一样 |  |
| Trace-user | 请求：  Data:  Ip=211.21.12.34\r\n  Starttime=12312412\r\n  Endtime=1231241412\r\n  应答:  Data:  Query1=2012:08:32:12 [www.xxx.com](http://www.xxx.com) A\r\n  Query2=2013:09:32:13 [www.yyy.org](http://www.yyy.org) mx; |  |
| Alarm | 请求:  Data:  Starttime=123124\r\n  Endtime=12314231\r\n  应答:  Data:  Alarm1=2012:08:32:12 QPS过大 |  |
| Alarm-stats | 请求:  Data:  Starttime=123124\r\n  Endtime=12314231\r\n  应答:  Data:  Alarm1=123456 3 867\r\n |  |
| Report | 请求:  Data:  Day=2012\08\09\r\n  Week=2012\34\r\n  Month=2012\03\r\n  应答:  url=sftp:\localhost\reports\213124.docx |  |

## 数据库

OPTION配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| Capture-filter | Varchar(256) |
| Capture-eth | Varchar(16) |
| Alarm-level | int |

VIEW配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| View-name | Varchar(16) |

match-client配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| Net | Varchar(32) |
| Viewid | int |

dns-server-list配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| ip | Varchar(32) |
| Viewid | int |

isp-net配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| ID | int autoincrement |
| Net | Varchar(32) |
| Viewid | int |

告警配置表

|  |  |
| --- | --- |
| 字段 | 类型 |
| Level | Int |
| Email | Varchar(32) |
| Mobile | Varchar(32) |