

---

爱思华宝统一通信

# 日志分析器向导

版本 10.4

**IceWarp**<sup>®</sup>





# 目录

<b>日志分析器</b>	<b>1</b>
快速启动.....	2
必需步骤.....	2
可选步骤.....	2
高级配置.....	5
日志导入器.....	6
常规.....	6
统计.....	8
本地化.....	9
外部日志查看程序.....	9
设置 & 用法.....	9
帮助.....	10
语言.....	10
数据库连接.....	10
查看器使用提示.....	10
远程查看器的使用(非服务器端).....	10
配置文件.....	11
没有 Raw 数据的会话日志导入.....	11
支持 & 排错.....	12
排错.....	12
支持 & 功能需求.....	12



## 第 1 章

# 日志分析器

爱思华宝服务器日志分析器是服务器引擎产生的日志文件统计和逻辑分析工具。

它的功能被分为两部份：

- 导入由服务器产生的纯文本日志文件到数据库。
- 通过运行数据库预设置或新建自定义查询生成统计图或报告，查看或发送到指定邮件。

每个功能都位于相应程序各自的界面内：

1. 从爱思华宝服务器管理员 GUI 内建的日志导入者(*mlaimp.exe*) 配置。  
从日志文件处理原始日志数据，并将信息以结构化记录的形式，存储到外部日志查看器应用程序的一个相应的 SQL 数据库中。
2. 外部日志查看器(*ILA.exe*)。  
这个独立的应用程序使用预设的和/或定制的 SQL 语句分析数据。

这种方法的优点是你能在熟悉的管理员 GUI 中完成所有的资料收集配置，允许爱思华宝服务器在晚上自动导入日志文件。同时日志查看器能被运行在任何外部机器上(比如你的台式机)，和连接到任一本地数据库的拷贝或远程数据库(需提供详细的连接数据)。

爱思华宝服务器日志分析器允许你快速并有效的分析服务器动作，哪怕早晨端着咖啡使用笔记本也能操作。



当前仅支持 SMTP、POP3、防病毒和防垃圾日志。

其它更多日志分析类型，以及增强的图表功能，文本 HTML 的统计和输出到 JPEG 和 PDF 等功能将在下个版本中提供。

## 本章内容

快速启动 .....	2
到处日志 .....	6
外部日志查看程序.....	9
Session Log without Raw Data Import .....	11
支持&排错.....	12

## 快速启动

日志分析器是安装后的一项重要功能。默认配置使用 MS Access 数据库存储数据，它完美适用于低数据流量的小型应用。大型应用需考虑使用一个企业级数据库解决方案，比如 MySQL 或者 MS SQL 。

使用 MySQL，需要从 <http://www.mysql.com/> 下载 MyODBC 3.51 版本驱动程序，创建一个日志分析使用的 DSN 和在它的数据库设置...对话框。



注意，您需要从 3.51 分支中下载 MySQL 的 ODBC 驱动程序 3.51.27.00 或较新的版本，5.x 版不支持。

进行以下操作开始收集和分析数据：

## 必需步骤

在主菜单的 帮助?许可证...菜单项，确认你的 日志分析器 模块许可证未到期。

(勾选 显示所有许可证 复选框以显示所有模块的许可证)

如果已到期，联系你的销售代表他将为您提供 30 天的试用许可证。

3. 在 系统 -- 服务 -- 常规 -- 服务 -- 日志 选项卡下，勾选 激活日志功能，并在 系统 -- 服务 -- 常规 选项卡选择 日志类型（调试，扩展等）。

注意：全局日志可以被启用 -- 使用 API 控制台 -- `c_system_logging_general_appendfiles` 变量。

4. 在 日志分析器 -- 常规，勾选 激活。

选择要处理的日志。

5. 在 日志分析器 -- 常规，导入数据。

日志会在每天凌晨 1:00 导入，因此现在你只能处理和分析前一天的日志，要查看和分析今天的日志，你需要使用 立即导入 按钮并选择你希望导入的日期。根据日志文件大小的不同所需时间可能不同。

注意 如果你想使用除 Ms Access（默认）之外的其他数据库，你需要在本步骤中预示好设置数据库。参考 [数据库设置](#) 部份获得更进一步信息。

6. 在 日志分析器 -- 常规，点击运行查看器按钮并查看你的数据。

爱思华宝日志分析器应用程序将打开 -- 当使用这种方式运行时，它将自动打开在 GUI 中配置的数据库。

7. 点击 应用 保存设置。

## 可选步骤

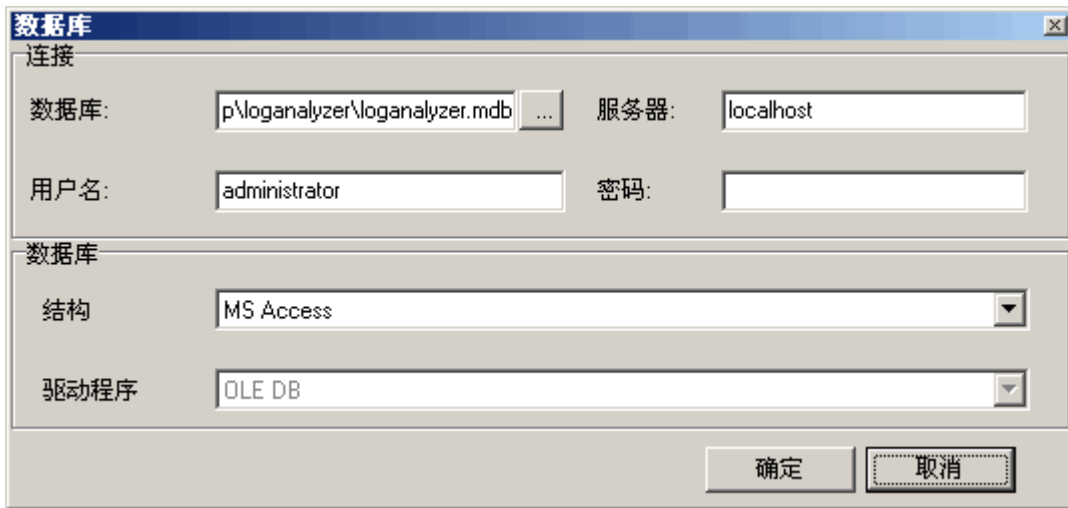
对于中型和大型安装，我们推荐使用 MySQL 或者 MS SQL 数据库代替 MS Access 。

### 数据库设置 Windows

1. 创建一个数据库。

用你的数据库管理员具创建一个空数据库。

2. 在 日志分析器 --常规 选项卡下点击 DB 设置 并配置连接到你刚刚创建创建的数据库。



注意，此处出现的对话框与爱思华宝服务器别的位置出现的标准对话框完全不同。

字段	描述
数据库	请确定你已正确的输入数据库文件的物理或 UNC 路径。 注意，"..." 按钮只有在选择 MS Access 语法时才有效。
服务器	输入 IP 或一个正式的域名。
用户名	输入用于连接到数据库的用户名。
密码	输入用于连接到数据库的密码。
语法	选择数据库的类型。
驱动程序	连接器到数据库。

3. 为测试连接，点击 立即导入 按钮后按下 确定，以打开 选择日期 对话框。
4. 转到日志目录并打开 `logalyzer\laYYYYMMDD.log` 文件以查看结果，你无需创建任何的 DSN 。

### 数据库设置 --- Linux

1. 安装 MySQL ODBC 驱动程序。

- On RHES 4.x

从 [rpm.pbone.net](http://rpm.pbone.net) 下载并安装 `mysql-connector-odbc`

取消 `/etc/odbcinst.ini` 文件中用于定义 MySQL 驱动程序行前的注释

**[MySQL]**

**描述 = ODBC for MySQL**

**//Driver = /usr/lib/libmyodbc.so** (聚集函数在 2.x 版本中不工作)

**Driver = /usr/lib/libmyodbc3.so** (检查该值，默认是错误的)

**Setup = /usr/lib/libodbcmyS.so**

**FileUsage = 1**

- On RHES 5.x

```
yum install mysql-connector-odbc
```

取消 `/etc/odbcinst.ini` 文件中用于定义 MySQL 驱动程序行前的注释

```
[MySQL]
```

```
描述 = ODBC for MySQL
```

```
Driver = /usr/lib/libmyodbc3.so (检查该值, 默认是错误的)
```

```
Setup = /usr/lib/libodbcmyS.so
```

```
FileUsage = 1
```

## 2. 创建 DSN

创建一个名叫 `ila` 的 DSN, 在用户主目录下的 `.odbc.ini` 文件内添加如下的部分内容(`/root/.odbc.ini`)

例子:

```
[ila]
```

```
描述= ILA
```

```
Driver= MySQL
```

```
Server= localhost
```

```
Database= ila
```

```
Port= 3306
```

```
Socket=
```

```
Option= 18435
```

```
Stmt=
```

```
User= root
```

## 3. 配置导入器

在 **日志分析器-常规** 选项卡下勾选 **激活** 选项框。

点击 **DB 设置** 按钮。

在 **数据库** 对话框的 **数据库** 字段填入 **DSN** 名称(在步骤 #2 中创建), 日志分析器将写入数据到它的数据表。

在 **服务器** 字段中填入运行 MySQL 的服务器地址(IP 或 FQDN)。

在 **用户名** 和 **密码** 字段填入用于连接到 MySQL 的证书。

设置 **combo MySQL** 语法。

例子:

```
Database = ila
```

```
Server = 127.0.0.1
```

```
User = ODBC
```

```
Password = ODBC
```

注意, 直到版本 9.4.1 为此, 控制台不能自动运行导入器, 要按计划导入数据你可以使用如下的 `shell` 脚本:

...



```
#!/bin/bash
# Launch the importer
export ICEWARDIR=/opt/icewarp
export PATH=/usr/bin:/bin:/usr/sbin:/usr/bin:$ICEWARDIR/loganalyzer
export LD_LIBRARY_PATH=/opt/icewarp/lib
export IWS_INSTALL_DIR=/opt/icewarp # Icewarp installation directory
export IWS_PROCESS_USER=root # User running the service
mlaimp
...
```

放置这些内容到/etc/cron.daily

启动导入器并检查日志。

## 高级配置

1. 导入完成后将产生一个导入日志状态概述邮件：

在 **日志分析器 -- 状态** 下，点击 **激活**。

输入你想发送概述的邮件地址。

选择你希望包含在报告中的概述日志的种类。

点击 **应用** 保存这些设置。

注意，该功能支持集群，可以从多个服务器中导入日志到同一个数据库中。

2. 要从如集群的多个服务器中导入日志到同一个数据库中：

在 **日志分析器 -- 常规 -- 选项**，设置 **服务器 ID** 属性以区别不同的服务器。

多个服务器的状态可以被存储到一个共同的数据库，并通过单个的查看器进行分析。在这种情况下每个使用导入器的副本都需要一个服务器许可证，而域管理员用于查看数据的查看器数量则没有任何客户端许可证的限制，无论你在服务器上或笔记本上使用。

要通过同一个查看器访问多个服务器的日志，只需要为所有服务器设备使用同一个数据库。只需要将各服务器的服务器 ID 标签选项设置为不同的值，系统即可支持负载均衡环境且可通过该值区分不同的服务器。

3. 查看完整服务：

在 **日志分析器 -- 常规 -- 选项**，点击 **导入 raw 会话 数据** 选项。

这将允许你查看到每个日志条目所有详细的服务会话信息，但同时这也将导致你的数据库大小增加。

4. 限制数据库的大小：

默认情况下系统会删除超过 7 天的日志记录以限制数据库的大小。具体的保存天数可以通过 **删除过期数据(天)** 选项设置。

5. 查看导入器相关活动的日志：

导入器相关活动的详细日志生成并保存在 **<安装目录>/loganalyser** 文件夹。

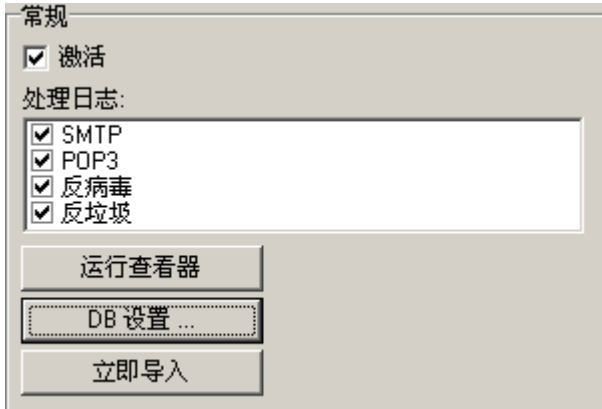
## 日志导入器

日志导入器是 "日志分析器"的服务器端接口。

它的目的导入纯文本日志文件到数据库，以允许你在大量数据堆积使用标准的 SQL 标准 查询。

一次性配置后它将在后台安静的运行。

### 常规



字段	描述
激活	检查该选项以激活日志文件导入处理。
处理日志	指定哪些日志你想导入。 <b>注意-日志必须被激活且应选择你想导入的相应日志类型，查看 <a href="#">系统 - 日志</a>。</b>
运行查看器	按下该按钮启动查看器应用程序，这可以让你以更友好的方式查看日志数据。
DB 设置	打开标准数据库设置对话框，定义日志分析器所使用的数据库和访问方式。 输入你需要访问数据库的结构(数据库类型)、用户名和密码。
立即导入	按下该按钮立即导入你的日志数据。 你通常不需要做这一步，导入会在每天 01:00 自动执行。 <b>注意 - 导入操作只导入前一天的数据。</b>

**选项**

导入 raw 会话数据

服务器 ID:

字段	描述
导入 raw 会话数据	<p>检查该选项以导入内存中的日志数据到数据库，允许你在查看器内以最初写入的格式查看数据，否则导入器只能从统计中捕捉到会话的数据。</p> <p>注意-该选项不会给你任何的额外的统计信息，仅能够从日志中查看已完成会话，并可能在自定义查询中使用这些记录。</p> <p>开启该选项将要导致你的数据库容量越来越大。</p>
服务器 ID	<p>可选办法，在数据上服务器名称。</p> <p>这些通常用于你有多个服务器，并且你将数据导入到同一个数据库，以便你能使用一台特殊服务器进行数据查询。</p>

**维护**

导入前清空数据表

删除过期数据(天)

字段	描述
导入前清空表格	<p>启用该选项将在导入以前从表格中删除所有的数据，因而任何时间你只能保留一天的数据(前一天的)。</p>
删除过期数据(天)	<p>启用该选项并输入一个数值以删除导入之前的老数据。</p> <p>这对于限制你的数据库容量是非常有用处的，并且确保你的分析器永远只分析几天内的数据。</p>
SQL 语句	<p>你能在删除数据前指定执行一组 SQL 语句。这些可用于，例如，生成一个查看数据的总计归档。</p> <p>按下按钮打开一位简易编辑框，你能在此处输入你的 SQL 语句。</p> <p>注意-该 SQL 语句仅在使用 "删去过期数据(天)" 选项时运行。</p>

## 统计

报告

激活

来自: admin@icewarpdemo.com

到: admin@icewarpdemo.com

统计:

SMTP

POP3

反病毒

反垃圾

字段	描述
激活	启用该选项，日志分析器将通过电子邮件方式投递综述报告。
From:	输入的电子邮件地址将做为报告的发件人。
To:	输入接收报告的收件人电子邮件地址。 可指定多个地址，用逗号进行分隔。
统计:	启用该选项指定你希望包含在报告中的统计项目。

日志分析器不会连接到本地主机发送报告邮件，报告邮件会提交到出站队列然后在 SMTP 处理后再投递它。

默认情况下，日志分析器连接到 127.0.0.1，你可以将 `[install_dir]\config\mla.dat` 文件中的 [STATS] 部份的 HOST 关键字进行修改。

例如

要使用 1.2.3.4 作为你的 SMTP，你需要修改 mla.dat:

**[GENERAL]**

.

.

**[STATS]**

**HOST=1.2.3.4**

## 本地化

从版本 10.2 开始，ILA 导入器允许通过替换 STRINGS 标签进行本地化。

你可以改变以下参数的值，位于 <install\_directory>\loganalyzer\rpt-lang.xml 文件：

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<LANGUAGE>
```

```
<STRINGS>
```

```
<STRING ID="MailSubject" VALUE="LogAnalyzer import statistics for server" />
```

```
<STRING ID="MailText" VALUE="Loganalyzer import statistics for server" />
```

```
<STRING ID="ReportTitle" VALUE="&lt;H1&gt;Loganalyzer import statistics for server %%SERVER_ID%% &lt;/H1&gt;
(processed at %%EXEC_TIME%% %%EXEC_DATE%%) &lt;BR&gt;" />
```

```
<STRING ID="ReportDateFormat" VALUE="dd/mm/yyyy" />
```

```
</STRINGS>
```

```
</LANGUAGE>
```



注意：改变任何东西的时候都必须遵循 XML 语法规则。

---

## 外部日志查看程序

外部日志查看器是日志分析器的用户界面，是真正进行日志分析的地方，在此我们可快速地查看服务器前一天的数据。

- 如果从爱思华宝服务器管理员 GUI 启动，它无须任何过多的设置即可工作。
- 如果作为独立的应用程序在另一台电脑上首次运行，你需要使用与服务器配置相同的设置，以连接到由日志导入程序创建的数据库。但需使用运行 DB 引擎的真实服务器的 IP 地址替代 localhost。

## 设置 & 用法

外部日志查看器应用程序能被运行在任何外部机器(比如你的台式机)，也能在指定详细的连接信息后连接到任一本地或远程数据库。

应用程序能在 <程序安装目录>\loganalyzer\ 被找到，名称为 ILA.exe。如果你希望从另一位置或机器运行，只需复制整个 loganalyzer\ 目录并运行 ILA.exe。

- 本地复制默认使用 MS Access 数据库，不需要进行额外设置。
- 如果你决定使用一个非默认数据库并在管理员 GUI 中配置了导入程序，你将需要改变连接，用运行 DB 的服务器 IP 地址以替代 localhost (如果从服务器继承设置)



注意-与爱思华宝服务器服务器不同，日志分析器是使用 OLE 连接到数据库，因此你仍然需要使用另外的对话框管理连接 -Windows 内建实用程序，用于选择数据库驱动程序，输入详细连接信息并测试连接是否工作。该对话框可以从 **菜单 -选项 -设置 - 连接** 并按高级 DSN 配置 按钮获得。

## 帮助

更进一步的使用帮助请在应用程序中按 F1。

## 语言

如果你希望切换界面到一个非英语语种，你可以选择 选项?语言，本地化语言会在新版本中不断增加。

## 数据库连接

要使查看器正常工作，你需要将其连接到用于处理统计数据数据库。它与导入器部份配置的数据库相同。

1. 选择 选项 -- 连接 -- 设置并选项相应的数据库类型。
2. 点击 内置 DSN 向导。
  - 如果你想使用默认的 MS Access 数据库，在<安装目录>/loganalyzer 文件夹下的 loganalyzer.mdb 文件，点击测试然后点击 OK。
  - 如果你想选择 MySQL 数据库 MS SQL，并且你已经建立了一个 DSN 且在管理员控制台中的导入器设置中已定义它，要完成 MLA 查看器的设置，你只需要在内置 DSN 向导输入同样的数据，点击测试然后点击 OK。

## 查看器使用提示

- 在 选项 -- 设置 -- 日历选项卡内，颜色方块表示每天导入的日志类型。
- SMTP 搜索功能非常强大，你可以执行如指定发件人、收件人和日志的搜索。为加快搜索速度，使用日期复选框指定搜索的时间段。
- 其它选项包括每 IP/域/用户的流量统计，POP3 搜索，会话期间统计和特殊查询。

## 远程查看器的使用( 非服务器端)

请注意，远程管理员控制台(可供下载)已经包含 MLA 查看器，但它必须重新配置数据库连接以便从远程工作，这包括在本地创建 DSN 并在管理员控制台和 MLA 查看器中设置 DSN。

如果你已经在远程服务器上配置了查看器的数据库连接，然后已经设置本地 DSN ，你可以只从远程服务器复制以下文件到本地控制台安装的同目录下：

```
<Installation Root>/config/mla.dat
```

你也可以复制整个/loganalyzer 文件夹到本地机器并运行 ila.exe 程序以启动查看器。

如果你希望从其他位置或机器运行，只需要复制整个 `loganalyzer\` 目录并运行 `ILA.exe`。

## 配置文件

默认的数据库连接超时时间是 300 秒。如果查询超过 5 分钟将被中止。你可以通过在 `<安装目录>/loganalyzer/mla_config.cfg` 配置文件中添加以下参数改变超时时间：

```
SQL_TIMEOUT = <timeout in seconds>
```

我们建议将该行添加到配置文件中任何其他记录的前面，比如 `DSN` 设置，查看以下示例，以下情况中，超时时间被设置为 10 分钟。

```
SQL_TIMEOUT=600
```

```
DSN=Driver={MySQL ODBC 3.51 Driver};Server=localhost;Database=icewarp_ila;UID=root;PWD=paassword;OPTION=2051
```

---

# 没有 Raw 数据的会话日志导入

导入器和查看器（版本 0.1.87 或更高）允许你在没有导入到数据库前查看一个会话的日志。

你需要：

- 在 **日志分析器 -- 常规** 选项卡禁用 导入 raw 会话数据
- 并导入一个新会话的日志。

要查看相应日志文件中会话的详细内容，必须激活查看器。现在你有两种方法实现它：

1. 在服务器（控制台），打开**查看器** -- 它将基于服务器设置自动查找。

或才：

1. 在一个客户端中，你可以复制本地日志文件：
  - - 在应该程序的基本路径下（`ILA.EXE` 执行程序所在的目录），创建 **Logs** 目录。
  - - 从服务器复制日志文件（`IceWarp/logs` 文件夹下）到该目录下的相应结构。

或在 `mla_config.cfg` 文件中添加 **LOG\_PATH** 设置使用户自定义的路径可用：

```
LOG_PATH=c:\storage\icewarp\logs;\\storage\icewarp\logs
```

当会话的详细信息无法发现时，查看器将显示（在 **会话详情中**）将显示之前的文件名和路径。

---

## 支持 & 排错

### 排错

大多数的常规错误由错误的数据库或数据库连接参数所造成。

你需要确认不同的数据库引擎有各种不同的配置

- 
- 数据库服务器已启动
- 数据库已创建
- 数据库包含一些数据
- "DB 设置.."对话框中是参数配置正确的

然后使用 "立即导入" 按钮重试导入并在任务管理器中寻找 **mlaimp.exe**，确定它是否已经运行。



如果问题没有涉及数据库或者你遇到的问题与基本 MS Access 数据库有关，通常最有效的解决方案是备份你有定制的文件，然后删除整个 Merak\logalyzer 目录，运行同样版本的爱思华宝服务器安装程序进行重新安装-这将得到全新的日志分析器和设置，不需要在服务器做任何修改。然后将定制文件/设置一个一个的复制回来，以隔离有问题的文件。

### 支持 & 功能需求

目前的日志分析器技术预展版不提供任何功能的保证，不过我们欢迎任何形式的反馈关于以下方面的问题：

- 稳定性问题
- 可再现的 BUG
- 你希望包含在安装程序的自定义查询
- 功能需求

在 <http://support.icewarp.cn> 提交一个请求并选择选项：

我需要帮助：日志分析器。