爱思华宝统一通信

日志分析器 - 查看器

版本 10.4

目录

第 1 章

日志分析器 - 查看器

爱思华宝日志分析器(ILA)是一个爱思华宝服务器生成地日志文件的统计和逻辑分析工具。

介绍

爱思华宝日志分析器处理日志文件并将处理后的记录重新组织存入 SQL 数据库，记录的活动可以使用日志查看器(ILA)应用程序查看监视，系统管理员可以为调试目的搜索特定事件或轻松改善系统效率。

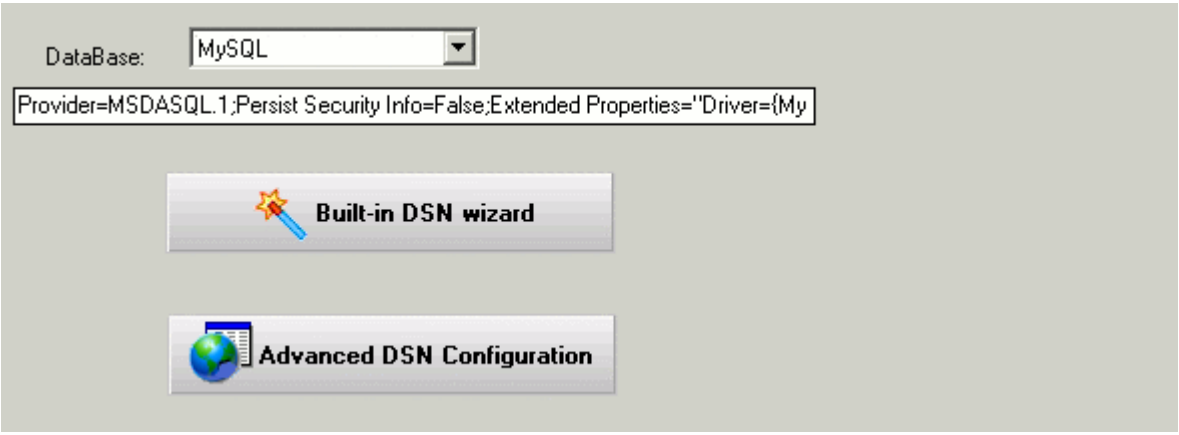
特别感谢：

Flávio Lucarelli of (巴西爱思华宝合作伙伴)
他的建议和帮助非常重要
非常感谢你 Flávio。

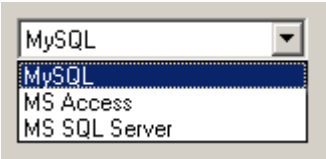
本章内容

入门指南

如果你以远程模式启动 ILA，你需要在启动后设置它的初始化配置。
ILA 使用一个外部数据库用于操作，因此你需要配置以连接到数据库。
数据库支持 MySQL、MS SQL 服务器和 MS Access ，你需要在这些数据库间作出选择。
如果你使用 MySQL 或 MS SQL 服务器，你需要在服务器上创建数据库并设置权限使 ILA 有权限访问数据库。
现在你需要配置数据库的连接。



选择你想使用的数据库



并点击 "建立 DSN 向导" 按钮。

一个窗口将打开并且你必须输入数据库的连接参数。

按下"测试" 按钮验证连接是否可以建立。

按下"确定" 关闭并确认已输入的参数。
按下"建立数据表" 按钮创建为存储日志数据的 ILA 数据表。
如果在该步骤中你遇到任何问题,则有可能是你的数据库访问限制不足以生成数据表，与你的数据库管理员联系寻求解决方案。
如果你使用 MySQL，参考 ***MySQL 疑难解答***。

本章内容

日志分析器配置

快速安装

1. 安装完成后如果你购选 **激活** 选项框（在 **日志分析器 -- 常规** 选项卡内)，默认的 MS Access 数据库将使用。
2. 在服务器上，你可以使用 立即导入 按钮开始导入 SMTP 日志。
3. 在日志分析器，**检查日志 - 导入处理**的结果。.
4. 启动查看器，在服务器，一个与导入器设置相同的默认的 DSN 将被创建（配置由爱思华宝 APi 准备）。

注意：“默认” 连接只有在查看器已启动但没有一个已定义的连接并在服务器上运行导入器时。

远程查看器用法

你不需要创建任何系统或基本 DSN 以使用爱思华宝日志分析器 -- 你只需要安装正确的 ODBC 驱动。

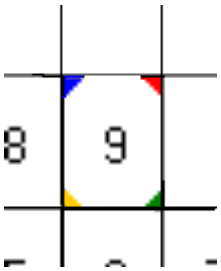
双击 **数据库连接 – 新建** 树项目并设置数据的相应参数，然后 **测试连接** 按钮测试连通性。

要查看已完成会话，你同样需要从远程机器复制 raw log 文件到本地位置。默认设置是在查看器所在位置的 logs 目录搜索 raw 文件。

导入日志文件

按下 ILA 工具栏中的 **导入** 按钮将打开 **导入** 窗口，可以看到三个选项卡：设置、日历和手动导入。

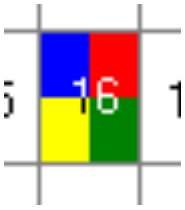
在日历选项卡你可以看到一个包含全年的日历，其中一些天数的四角有些不同颜色的区块。



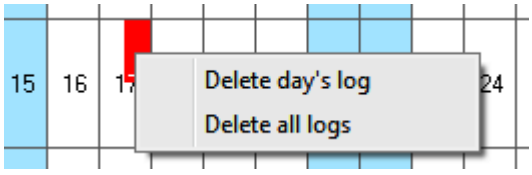
转角颜色表示在基本日志目录中已有显示天的日志文件。
不同的颜色表示不同的日志文件类型：

- 蓝色表示 SMTP 日志文件；
- 红色 表示 POP3 日志文件；
- 黄色表示反病毒日志文件；
- 绿色表示反垃圾邮件日志文件；

日志文件导入后颜色将改变并占据当天的全部面积(或正方形)象如下图像：



右键单击一天你将得到一个弹出菜单，你可以选择删除所选天的日志或删除所有日志。



单独 SMTP 日志

要单独导入一个 SMTP 日志， 双击 数据库连接 -- **<internal>** -- 导入的左面板树条目，通用的 打开 对话框允许你浏览一个单独的 SMTP 日志文件。

导入当前天的日志

要导入当前天的日志，你可以创建一个批处理文件带 -**dtoday** 开关。

注意：如果一个 SMTP 会话出现跨越两天的情况发生（例如开始于 23：58，结束于第二天的 00：03），ILA 将不会显示其为一个单独的会话，只有相应天的会话会被显示。

IP 统计

使用 "IP 统计"你能获得指定 IP 地址来自或目的的原始流量的相关信息。

对于每个远程 IP 地址，以下信息都将显示：

次数	通过爱思华宝邮件服务器处理的邮件总数。
大小	邮件总大小（MB）。
持续时间	所有会话的持续时间总数，表示为 hh:mm:ss。
失败	失败邮件数量。
成功	邮件成功投递的数量。

使用常用过滤器你能集中显示日志的某一部份或某些类型。

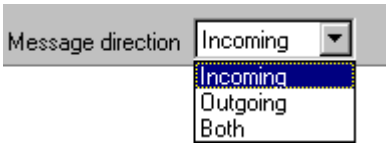
域统计

"域统计"返回有关发送域或本地域的原始流量信息。对于每个域将显示以下信息：

次数	通过爱思华宝邮件服务器处理的邮件总数。
大小	传送数据的大小（单位：MB）。
持续时间	所有会话持续时间的总和，表示为 hh:mm:ss。
失败	失败邮件数量。
成功	邮件成功投递的数量。

使用常用过滤器你能集中显示日志的某一部份或某些类型。

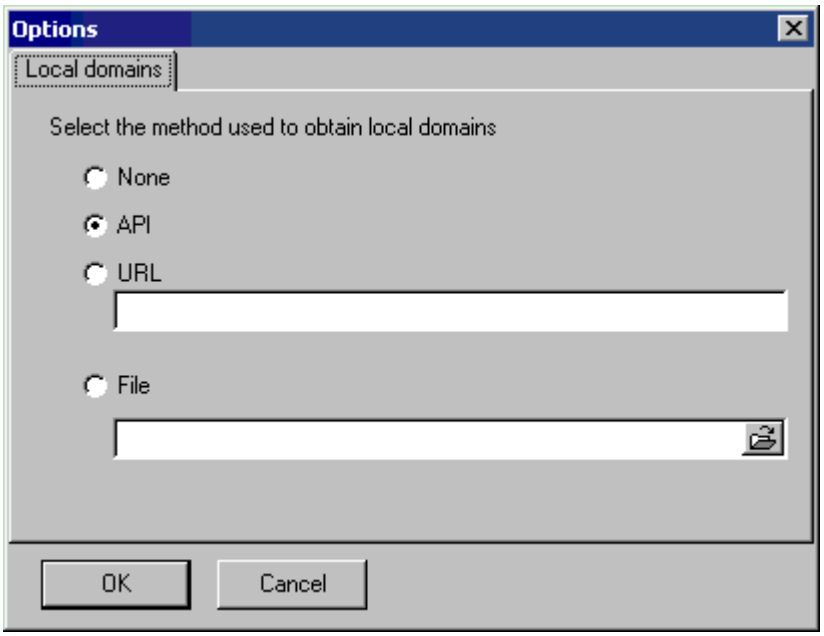
你可以使用邮件方向器选择器筛选结果，



用来限制只报告收到，发出或两者的邮件。

如果只过滤本地域邮件，使用 “仅本地域”。

要使用这些选项，你必须配置来自爱思华宝邮件服务器的本地域列表。这个列表可以在许多方面获得。要配置如何使用选项窗口获得本地域列表：



该选项是：

API	如果 ILA 和爱思华宝邮件服务器安装在同一台机器，你能使用爱思华宝 API 获取本地域列表。这是最简单的方法。
URL	一个 web 页面返回包含一列域的页面。通常如果 ILA 没有安装在爱思华宝邮件服务器上时，该页面可以由爱思华宝整合的 Web 服务器提供。
文件	一个简单的 ASCII 文本文件，包含一个每列一行的域列表。一般用于之前两种方式无法实施的情况下。 爱思华宝邮件服务器提供一个工具用于导出域列表，在爱思华宝邮件服务器帮助中查找 **"tool.exe "**。 用法： *tool.exe export domain * > file_list.txt*

用户统计

用户统计关于来自或地址到本地帐户的原始流量的返回信息。

每个用户的返回信息是：

次数	通过爱思华宝邮件服务器处理的邮件总数。
大小	传送数据的大小（单位：MB）。
持续时间	所有会话持续时间的总和，表示为 hh:mm:ss 。
失败	失败邮件数量。
成功	邮件成功投递的数量。

使用常用过滤器你能集中显示日志的某一部份或某些类型。

全局

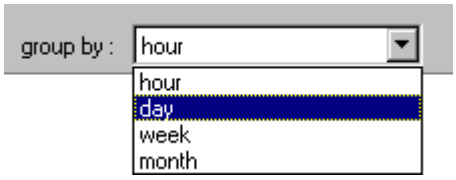
全局 统计显示有多少邮件成功投递，多少邮件被拦截以及为什么被拦截。

邮件分类为：

OK	该邮件被正确投递。
DNSBL	会话因为 "DNS 黑名单"过滤器被拒绝。发件人的 IP 地址由于发送垃圾邮件或其他恶意的动作被禁止。
ANA	邮件被拒绝因为发件人没有访问许可(访问不被允许）。
AS	邮件因为反垃圾邮件被拒绝。
AV	邮件被反病毒检查。
DBF	邮件被 "过滤器删除"。这通常是一个内容过滤器。
SDME	邮件因为发件人的域不存在而被拒绝(发件人的域必须存在)。
SCAN	一个入站连接已经建立但是没有邮件投递的尝试。这是典型的端口和服务扫描工具。
TARP	始发 IP 地址通过爱思华宝服务器被拦截，因此投递会话被拒绝。拦截现在由侵入预防完成。
WDNR	邮件被拒绝因为中继到最终收件人不被允许（我们不允许中继）。
UNK	邮件被拒绝因为收件人地址不存在(用户未知)。
CNC	一个客户端会话失败因为爱思华宝服务器不能连接到远程 SMTP 服务器(不能连接)。
ERROR	邮件由于有些未知错误没有投递。
CA	邮件被接收并转发到一个监控邮箱 - 所有地址(监控所有帐户)。
INCPLT	会话不完整。
GRLST	邮件被灰名单拒绝。

该表格报告会话数量或邮件成功以及被拒绝的原因。

你能通过选择 "分组依据" 选择器每小时，每天，每周或每月获得一个报告。



使用 通用过滤器 你能集中处理一部份被记录的数据。

报告生成后，你能在相应位置使用加亮阈值选项轻松突出显示你关注的内容，高于阈值的值将加亮显示。

以图显示在服务器上有多少 SCAN 和 UNK 相关的活动被分析。

Hour	Processed	Succeeded	ANA	AV	DBF	DNSBL	SDME	TARP	UNK	SCAN	WDNR	CNC	ERROR
2005-12-18 00:00:00	1770	258	156	18	6	432	6	30	306	498	0	0	0
2005-12-18 01:00:00	1332	210	4	0	6	310	0	20	292	474	0	0	4
2005-12-18 02:00:00	1016	207	10	4	16	167	8	7	330	228	0	0	0
2005-12-18 03:00:00	702	78	15	3	3	165	6	0	171	252	0	0	0
2005-12-18 04:00:00	711	102	12	9	0	117	6	12	183	240	0	0	0
2005-12-18 05:00:00	753	168	0	0	0	147	9	15	204	201	0	0	0
2005-12-18 06:00:00	354	48	17	2	3	73	4	2	66	125	0	0	0
2005-12-18 07:00:00	179	57	0	0	1	33	0	2	34	51	0	0	0

使用百分比按钮"%"，你可以在不同的值之间切换，凡是信息的值与邮件总数之间的比例在该百分比之上的都会加亮显示以便于你的分析。这通常用于评估每个值/项目的重要性。

邮件搜索

这强力的搜索工具能被用于多个任务，比如：

搜查一个指定邮件和查看，如果它被接收或被拒绝的理由。

详细分析每个域/用户的接收和发送流量。

搜查匹配指定条件的邮件投递会话。

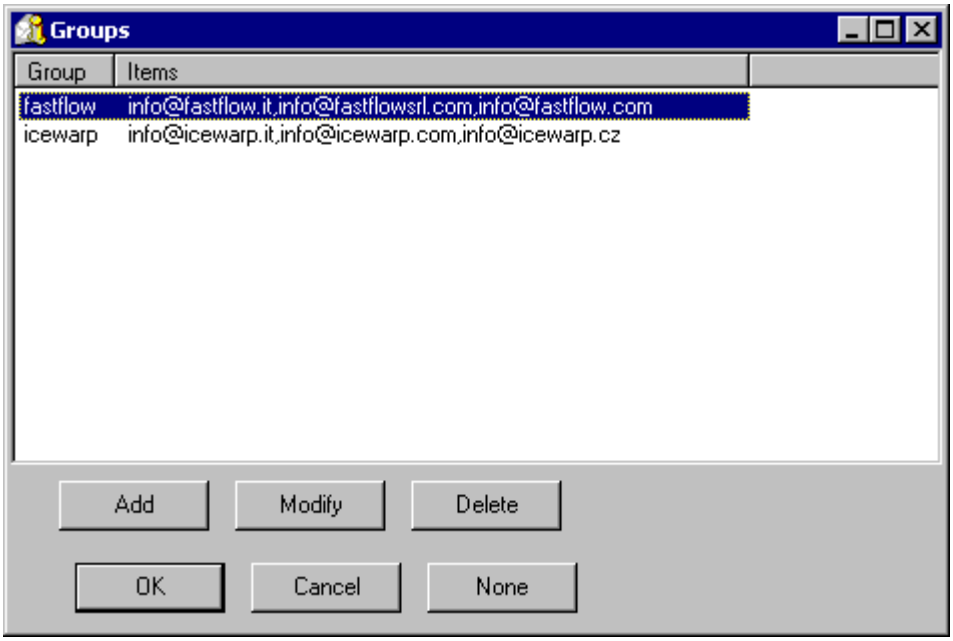
除了标准的 **通用过滤器** 以外你还能指定以下过滤器：

From account	"MAIL FROM "地址的别名
From domain	"MAIL FROM "地址的域名
To account	"RCPT TO "地址的别名
To domain	"RCPT TO"地址的域名

使用 通用过滤器 你能集中处理一部份被记录的数据。

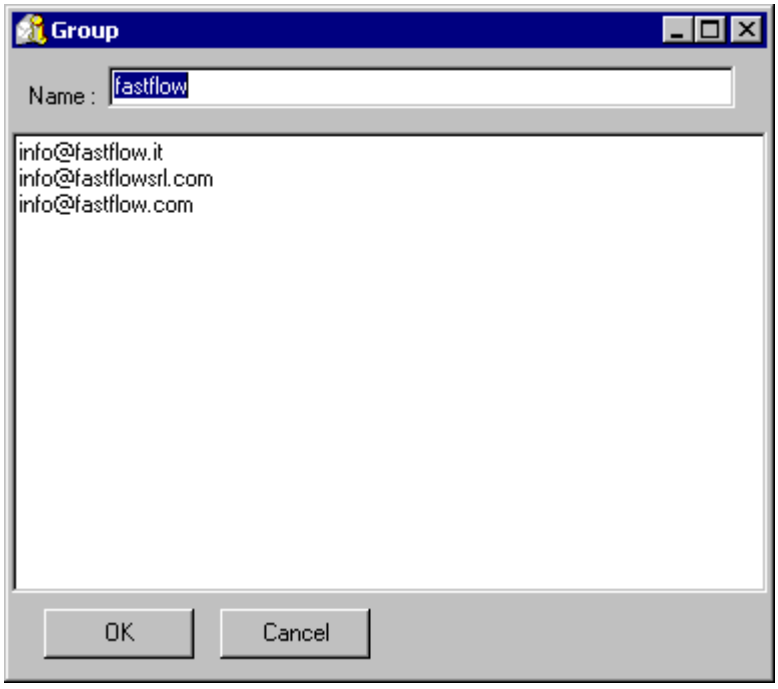
使用列表按钮  你能列出所有可用的 **from/to** 帐户或 **from/to** 域并选择你需要的项目。

为了在多个域或帐户中进行筛选，你可以创建组值。单击组按钮  组管理员将显示：



在这里你可以添加，删除或修改组。

组是被过滤的日志数据的邮件地址列表。



你能根据会话结果进行筛选。

你能在本向导的全局统计 部分了解这些缩写的详细说明。

直接搜索方式

要搜索你需要的：

1. 在左侧面板选择 ***直接搜索***。
2. 使用"..." 按钮选择日志文件。
3. 输入搜索关键字，然后按下右边按钮开始搜索字符串，搜索字符串不支持正则表达式，你不能使用 “*”或其他特殊字符。

   有效的搜索字符串示例如下：

*** – 搜索日志中所有会话；

Client session – 搜索所有客户端会话；

@icewarp.com.br – 搜索所有包含"@icewarp.com.br" 的会话；

4. 现在你可以使用 ***From*** 和 ***To*** 过滤器优化你的搜索。如果你想过滤以前的搜索，你应该按下的左侧的播放按钮。

如果你在一行上右击，你可以根据 ***Message ID*** 搜索并查看该邮件的整个处理过程。搜索的时间与结果的行数成正比。（尝试一个大的 LOG 文件（50MB – 约 8000 行）搜索时间小于 200 ms），如果你右击一个会话，你将看到 ***搜索 MessageID*** 功能。

在同一个上下文菜单中，你可以看到整个会话，你可以解码 ***base64*** 字符串，复制并选择一个；你可以在会话中选择一个字符串，如果它能被解码，当你停止移动鼠标时，将会显示一个提示。

你也可以创建一个***本地 MySQL*** DSN – 使用本设置，你将获得更快的响应时间，并且不需要 ***libmysql.dll*** 连接到数据库。

持续时间统计

持续时间 部分提供有关邮件处理所需时间的详细信息，通过相应会话的结果分类和群组。

时间表示为 **hh:mm:ss** 。

统计显示为：

MinDuration	一个类别邮件的最小处理时间
MaxDuration	一个类别邮件的最大处理时间
AvgDuration	一个类别邮件的平均处理时间
SumDuration	该类别的总处理时间
SumSize	所有会话数据传送期间的总时间数

这些统计数据有助于了解总体负载的分布以及爱思华宝服务器的过滤器和安全系统是有效的或需要进一步调整。

使用 通用过滤器 你能集中处理一部份被记录的数据。

自定义搜索

如果你需要分析一些特定的问题并且默认统计数据无法适合你的需要，你可以访问存储在 ILA 数据库中的数据并构造自己的 SQL 查询来提出任何种类的信息。特定参数可以被包含在 SQL 语法中以提高筛选结果的准确性，参数为你提供指定的输入字段。

参数语法：
:[*parameter_name[:default_value[:parameter_type[:parameter_format]]]****]***

范例 1:

```
SELECT * FROM smtp WHERE lg_FromDomain=:[Domain]
```

上述范例中参数 "Domain" 替换了 "来源域名"的静态值。

范例 2:

```
SELECT * FROM smtp WHERE lg_FromDomain=:[Domain:icewarp.it]
```

上述范例中参数 "Domain" 替换了一个 "From Domain"静态值并设置缺省值为 "icewarp.it"。.

范例 3:

```
SELECT * FROM smtp WHERE lg_Duration>:[Min Duration:100:integer]
```

上述范例中参数 "Min Duration" 替换一个 "Duration" 静态值并设置缺省值为 "100"。它声明该参数为整型，因此你得到一个整数值编辑框。

范例 4:

```
SELECT * FROM smtp WHERE lg_Date>':[Since:07/06/2005:Date]'
```

上述范例中参数 "Since" 替换了一个 "Date"静态值并设置缺省值为 "07/06/2005"。它申明该参数为日期类型,因此你将得到一个日历编辑框。

范例 5:

```
SELECT * FROM smtp WHERE lg_Date>':[Since:07/06/2005:Date:yyyy-mm-dd]'
```

上述范例中参数 "Since"替换一个 "Date"静态值并设置缺省值为 "07/06/2005"。它申明该参数作为日期类型,因此你将得到一个日历编辑框。该参数值用于 SQL 命令的格式是 "yyyy-mm-dd" 以匹配指定数据库的需求。

数据库表和字段

ILA 数据表

日志数据以下列结构存储在数据库的数据表中：

SMTP 表

lg_AI recordID	记录的 ID
lg_ATRN	ATRN 命令执行时的域名
lg_ATRN_res	**ATRN** 命令执行时的结果： **"N"**不是一个 ATRN 会话； **"S"**有该域下的邮件； **"F"**该域下没有任何邮件；
lg_AUTH	**AUTH** 命令执行的结果： **"N"**没有出现验证； **"S"**用户验证成功； **"F"**验证失败；
lg_AV	反病毒响应如果投递的邮件包含被感染的内容。
lg_AccessNotAllowed	**"Y"**邮件被黑名单或 helo 过滤器阻止； **"N"**该条件没有应用；
lg_ClientSession	**"Y"**会话是一个客户端会话； **"N"**会话是一个服务器端会话；
lg_DNSBL	如果存在，表示该主机名所在的 DNSBL 系统已经将发件人的 IP 地址列入黑名单。
lg_Date	会话的日期.
lg_DeletedByFilter	如果存在，表示该名称的过滤器拒绝了本邮件。
lg_DomainSenderMustExist	**"Y"**,邮件被拒绝因为发件人域不存在。
lg_Duration	会话持续的秒数。
lg_ETRN	哪些域的 ETRN 命令被执行。
lg_Error	"**OK**"没有错误发生； 否则可能是以下任意一个值 **"TARP","ANA","UNK","SDME","SCAN","AV","DNSBL","DBF","WDNR","ERROR".**

lg_FromAccount	发件人的别名。
lg_FromDomain	发件人的域。
lg_FromIP	远程系统的 IP 地址。
lg_Helo	如果存在，这是提交到服务器的 HELO 值。
lg_Incomplete	**"Y"**会话没有完成； **"N"**会话正确完成。
lg_Log	Raw 会话数据，用 ZLib 算法压缩。
lg_LogRows	Raw 会话数据行次数。
lg_MessageID	Message ID，如果任何邮件已经接收。
lg_Relay	**"N"**邮件没有被中继或中继被拒绝； **"Y"**邮件成功中继。
lg_Scan	**"PROT"**远程系统仅询问服务器能力并断开连接。 **"PORT"**没有真实会话出现，该远程系统仅仅连接并断开。 **"N"**该会话是一个正常会话。
lg_Server	服务器 ID。
lg_Size	邮件的大小字节数。
lg_TLS	响应一个 TLS 指令： **"N"**没有 TLS 请求； **"S"** TLS 指令成功完成； **"N"** TLS 指令报告一个错误。
lg_TS	通过 ILA 处理日志的时间戳
lg_Tarpitting	**"Y"**远程 IP 地址被拦截系统拒绝； **"N"**拦截没有触发或没有激活。
lg_ThreadID	连接的线程 ID 。
lg_Time	连接的启动时间。
lg_ToAccount	收件人的别名。
lg_ToDomain	收件人的域。
lg_UserUnknown	**"Y"**目的地址在服务器不存在； **"N"**目的地址被服务器接受。

POP3 表

pop_AI	记录 ID。
pop_Server	服务器 ID 。
pop_ThreadID	连接的线程 ID 。
pop_FromIP	远程系统的 IP 地址。
pop_Date	会话的日期。
pop_Time	连接的启动时间。
pop_Duration	会话持续的秒数。
pop_RETR_Count	从服务器上接收的邮件数。
pop_RETR_Size	从服务器检索邮件的总大小。
pop_DELE_Count	删除邮件数。
pop_AUTH	**AUTH** 命令执行的结果： **"N"**命令没有提交； **"S"**验证成功； **"F"**验证失败。
pop_Account	邮箱的用户名。
pop_Password	邮箱的密码。
pop_Log	Raw 会话数据，用 ZLib 算法压缩。
pop_LogRows	Raw 会话数据行次数。
pop_MsgSize	包含在邮箱中的邮件大小。
pop_MsgCount	包含在邮箱中邮件的数量。
pop_Error	假如失败时的错误。
pop_ClientSession	**"Y"**客户端会话(远程帐户)； **"N"**正常的 POP3 会话；

反垃圾表

as_AI	记录的 ID

as_Server	服务器 ID 。
as_ThreadID	连接的线程 ID
as_FromIP	远程系统的 IP 地址。
as_FromAccount	发件人的别名。
as_FromDomain	发件人的域。
as_Date	会话的日期。
as_Time	会话开始的时间。
as_MessageID	邮件 ID。
as_Log	Raw 会话数据，用 ZLib 算法压缩。
as_LogRows	Raw 会话数据行次数。
as_ToAccount	收件人的别名。
as_ToDomain	收件人的域。
as_Score	垃圾邮件总得分。
as_Action	服务器执行的动作。
as_RSBody	以下特征码的值： *Parts = 0x0001* *External = 0x0002* *NoText = 0x0004* *Script = 0x0008* *Differ = 0x0010* *NoBodyNoSubject = 0x0020* *Filters = 0x0040*
as_RSByPass	以下特征码的值： *License = 0x0001* *WhiteList = 0x0002* *Trusted = 0x0004* *Outgoing = 0x0008* *Size = 0x0010* *Bypass = 0x0020* *NoUser = 0x0040* *Mode = 0x0080*
as_RSCharset	以下特征码的值： *CharsetFilter = 0x0001* *CharsetMissing = 0x0002*
as_RSBayes	贝叶斯过滤器得分。

as_RSSpamAssassin	垃圾杀手得分。
as_RSBW	**"Y"**黑&白名单已经应用； **"N"**没有黑&白名单是包括；
as_RSContentFilter	**"Y"**一个内容过滤器已经被应用； **"N"**没有内容过滤器包括；
as_RSStaticFilter	**"Y"**一个静态过滤器被该动作影响； **"N"**没有静态过滤器应用；
as_RSChallengeResponse	**"Y"**挑战/响应已经被应用； **"N"**挑战/响应没有应用；

反病毒表

av_AI	记录 ID。
av_Server	服务器 ID 。
av_ThreadID	连接的线程 ID 。
av_FromIP	远程系统的 IP 地址。
av_FromAccount	发件人的别名。
av_FromDomain	发件人的域。
av_Date	会话的日期。
av_Time	会话开始的时间。
av_MessageID	邮件 ID.
av_Log	Raw 会话数据，用 ZLib 算法压缩。
av_LogRows	Raw 会话数据行次数。
av_ToAccount	收件人的别名。
av_ToDomain	收件人的名称。
av_Virusname	发现病毒的名称。
av_Filename	包含病毒文件的名称。

Mysql 调试

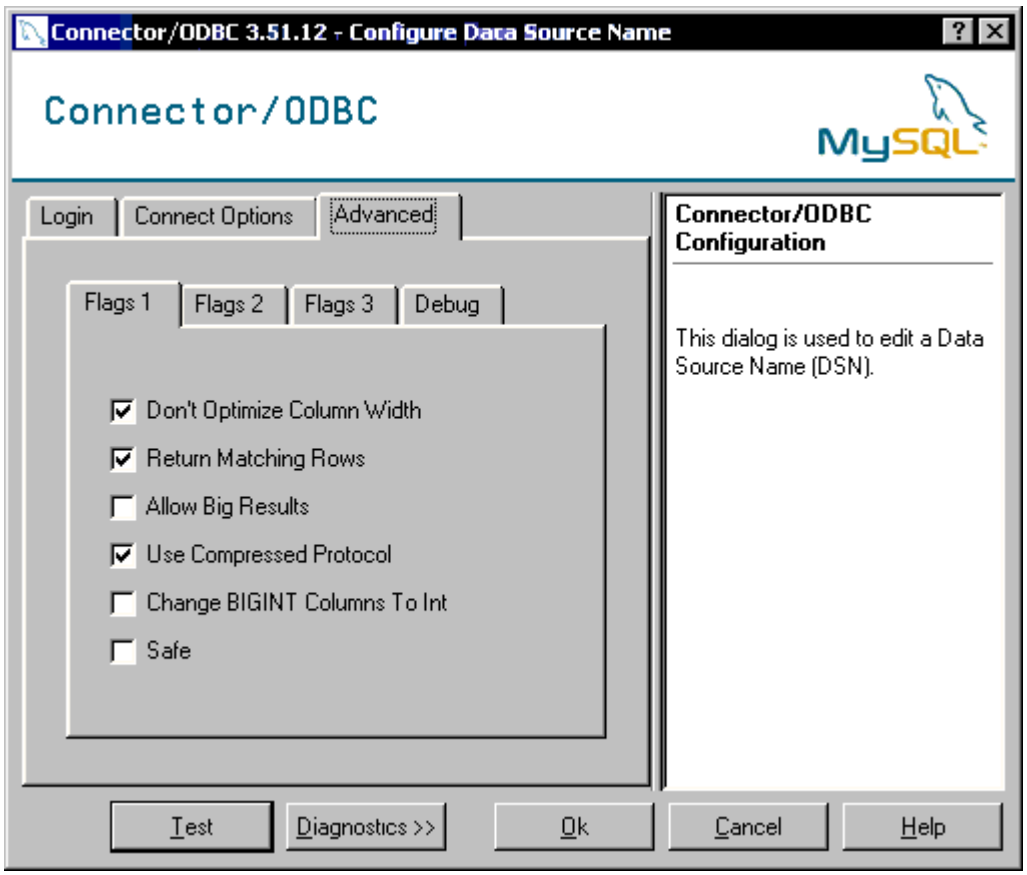
配置 MySQL 外部 DSN

如果你没有使用内部的 DNS 配置(推荐使用它)，适当调整你的 ODBC 驱动程序选项非常重要。

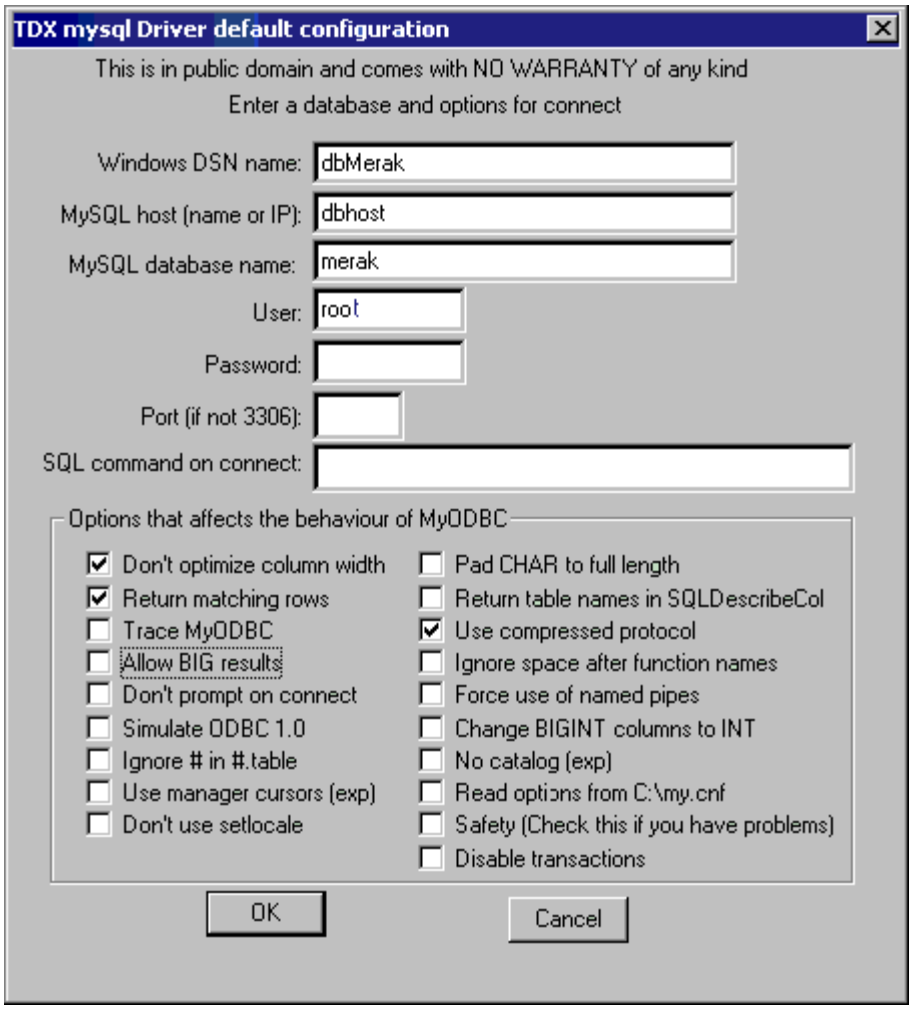
ILA 有一个编辑器用于帮助你配置 ILA 导入工具。
如下所示，配置一个正常的 DSN 选项用于访问 MySQL：

不要优化列宽
返回匹配行
使用压缩协议

如果你使用 MySQL ODBC 驱动程序 3.51.XX ，你的配置看来像如下截图。



如果你使用 MySQL ODBC 驱动程序 2.50.XX，你的配置看来像如下截图。



MySQL 服务器版本 5.00 或者更新版本

如果你的 MySQL 服务器版本是 5.00 或者更新的，你必须使用 MySQL ODBC 驱动程序 3.51.12 或者更新版本以便 ILA 能够工作。

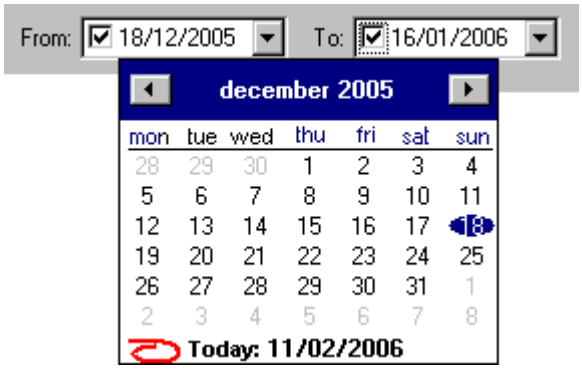
注意相关信息。

通用过滤器

通用过滤器 有助于减少在报告中显示的数据量，当你需要把重点放在一个特定的时间间隔或一个指定发件人/收件人时这非常有用。

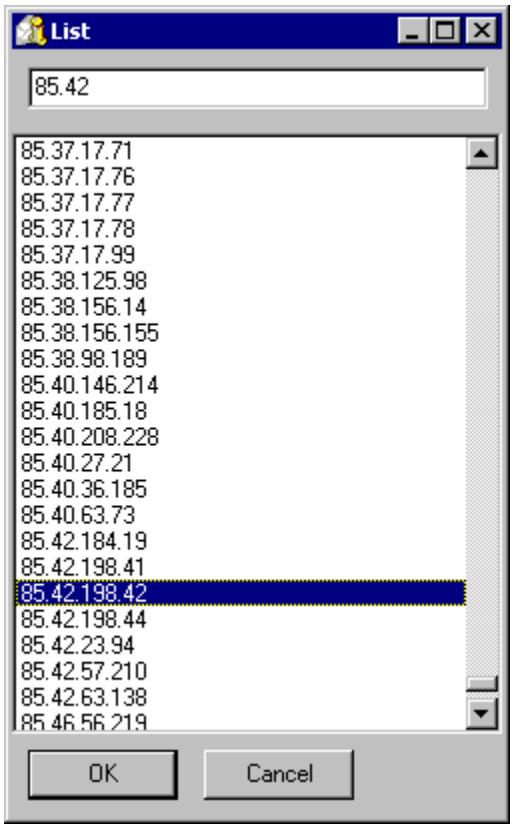
你能过滤：

- 日期，指定的时间间隔，只有在这个日期之间的日志信息被用于生成报告。

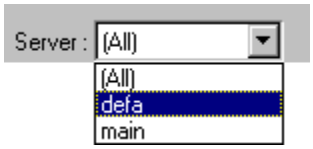


- IP 地址，输入你在需要分析的活动 IP 地址，或直接从下拉框选择 "IP "值。

  使用按钮  列出在数据库中存在所有 IP 地址，也为通过输入前几个数字，搜索一个特定的地址。



服务器使用 "***服务器***" 选择器。



- 会话类型(客户端、服务器端或两者)使用 "会话类型" 选择器(查看 爱思华宝邮件服务器手册更多有关客户端/服务器连接的信息)。