日志记录

本章包含以下部分：

概述

了解日志文件和日志订用

日志是收集 AsyncOS 邮件操作重要信息的有效方法，非常节省空间。这些日志将记录邮件网关上发生的活动的相关信息。日志中的信息会因您查看的日志（例如，退回日志或传送日志）而异。

大多数日志采用纯文本(ASCII)格式记录；但为保证资源效率，传送日志采用二进制格式。ASCII 文本信息在任何文本编辑器中均可读。

思科提供 M 系列思科安全管理器邮件和网络网关，作为来自多个邮件网关的日志的集中报告和跟踪工具。请联系您的思科代表，了解详情。

日志订用可将日志类型与名称、日志记录级别和其他约束（例如大小和目标信息）关联起来；同一日志类型允许存在多个订用。

日志类型

日志类型指明了在生成的日志中记录的信息，例如，消息数据、系统统计信息、二进制或文本数据。创建日志订用时，您可选择日志类型。有关详细信息，请参阅日志订用, on page 66。

AsyncOS 会生成以下日志类型：

Table 1: 日志类型

记录	说明
文本邮件日志	文本邮件日志记录邮件系统操作的相关信息。例如，邮件接收、邮件传送尝试、打开和关闭的连接、退回、TLS 连接等。
qmail格式邮件日志	qmail格式传送日志记录的邮件系统操作信息与下文中的传送日志相同，但会将信息存储为 qmail 格式。
投递日志	传送日志记录邮件网关的邮件传送操作的重要信息，例如，有关每次收件人传送的信息以及传送尝试时的退回相关信息。日志消息为“无状态”消息，这意味着所有相关信息都会逐条记录在每条日志消息中，用户无需参考上一条日志消息即可了解当前传送尝试的相关信息。传送日志以二进制格式记录，以提高资源效率。必须使用提供的实用程序对传送日志文件进行后处理，将其转换为 XML 或 CSV（逗号分隔值）格式。转换工具位置： https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools
反弹日志	退回日志记录有关退回的收件人的信息。为每个退回的收件人记录如下信息：邮件 ID、收件人 ID、封信发件人地址、信封收件人地址、收件人退回的原因以及来自收件人主机的响应代码。此外，针对每个退回的收件人邮件，您还可以选择记录固定大小的信息。此大小以字节为单位，默认为零。
状态日志	此类日志文件记录 CLI 状态命令中的系统统计信息，包括 status detail 和 dnsstatus 命令。记录期限使用 logconfig 中的 setup 子命令设置。状态日志中的每个计数器或记录的速率为从上次重置计数器起至当前的值。
域名调试日志	域调试日志记录邮件网关与指定收件人主机之间的SMTP会话期间的客户端和服务器通信。此类日志可用来调试特定收件人主机存在的问题。必须在日志文件中指定要记录的 SMTP 会话总数。随着会话记录的增加，此数目会逐渐减少。可以通过删除或编辑日志订用，在记录所有会话之前停止域调试。
注入调试日志	注入调试日志记录邮件网关与连接到系统的指定主机之间的 SMTP 会话。注入调试日志对于排除邮件安全设备和互联网上某主机之间的通信问题很有帮助。
系统日志	系统日志记录以下信息：引导信息、虚拟邮件网关许可证到期警报、DNS 状态信息和用户使用 commit 命令输入的备注。系统日志对于排查邮件网关的基本状态很有用。
CLI审核日志	CLI 审核日志会记录系统中的所有 CLI 活动。
FTP服务器日志	FTP 日志记录了有关在接口上启用的FTP服务的信息。会记录连接详细信息和用户活动。
GUI 日志	请参阅 HTTP 日志。

记录	说明
HTTP日志	HTTP 日志记录接口上启用的 HTTP 和/或安全 HTTP 服务的相关信息。由于图形用户界面 (GUI) 通过 HTTP 访问，因此 HTTP 日志实质上等同于CLI审核日志的GUI。日志会记录会话数据（新会话和过期的会话）和在 GUI 中访问的页面。 这些日志还包括有关SMTP事务的信息，例如，从邮件网关上邮件发送的计划报告的信息。
NTP 日志	NTP 日志记录邮件网关与配置的所有 NTP（网络时间协议）服务器之间的会话。有关详细信息，请参阅“系统管理”章节的“编辑网络时间协议 (NTP) 配置（计时方法）”部分。
LDAP调试日志	LDAP 调试日志用于调试LDAP安装。（请参阅“LDAP 查询”一章。）此类日志将记录有关邮件网关发送到LDAP服务器的查询的实用信息。
反垃圾邮件日志	反垃圾邮件日志记录系统反垃圾邮件扫描功能的状态，包括最新反垃圾邮件规则更新的接收状态。此外，日志还将记录所有与情景自适应扫描引擎相关的日志。
反垃圾邮件归档	如启用反垃圾邮件扫描功能，此类日志将存档经过扫描且与“存档邮件”操作有关的邮件。日志文件为 mbox 格式。有关反垃圾邮件引擎的详细信息，请参阅“反垃圾邮件”一章。
灰色邮件引擎日志	包含有关灰色邮件引擎、状态、配置的信息等。大多数信息处于信息或调试级别。
灰色邮件存档	包含存档的邮件（经过扫描且与“存档邮件”操作关联的邮件）。日志文件为 mbox 格式。
防病毒日志	防病毒日志记录系统防病毒扫描功能的状态，包括最新防病毒身份文件更新的接收状态。
防病毒归档	如启用防病毒引擎，此类日志将记录经过扫描并与“存档邮件”操作关联的邮件。日志文件为 mbox 格式。有关详细信息，请参阅“防病毒”一章。
AMP 引擎日志	AMP引擎日志记录系统高级恶意软件防护功能的状态。有关详细信息，请参阅文件信誉过滤和文件分析：
AMP 存档	如已将邮件策略配置为对高级恶意软件防护引擎发现附件不可扫描或包含恶意软件的邮件进行存档，此类邮件会存档至此处。日志文件为mbox格式。
Scaning 日志	扫描日志包含扫描引擎的所有LOG和COMMON消息（请参阅警报）。这类消息通常是应用故障、发送的警报，失败的警报和日志错误消息。此日志不适用于系统范围警报。

记录	说明
垃圾邮件隔离区日志	垃圾邮件隔离区日志记录与垃圾邮件隔离区进程相关的操作。
垃圾邮件隔离区 GUI 日志	垃圾邮件隔离区日志记录与垃圾邮件隔离区相关的操作，例如，通过 GUI 进行的配置、最终用户身份验证和最终用户操作（发行邮件等）。
SMTP 会话日志	SMTP 会话日志记录传入和传出 SMTP 会话的所有信息。
安全/阻止列表日志	安全列表/阻止列表日志会记录有关安全列表/阻止列表设置和数据库的数据。
报告日志	报告日志会记录与集中报告服务的进程相关的操作。
报告查询日志	报告查询日志会记录与邮件网关上运行的报告查询相关的操作。
更新程序日志	更新程序日志记录与系统服务更新相关的事件，例如 McAfee 防病毒定义更新。
跟踪日志	跟踪日志记录了与跟踪服务过程关联的操作。跟踪日志是邮件日志的子集。
身份验证日志	身份验证日志记录成功的用户登录和失败的登录尝试。
配置历史记录日志	配置历史记录日志记录以下信息：邮件网关上发生的变更以及变更发生的时间。每次用户提交更改时，都会创建一份新的配置历史记录日志。
升级日志	有关升级下载和安装的状态信息。
API 日志	API 日志记录与邮件网关 AsyncOS API 相关的各种事件，例如： • API 启动或停止 • 到 API 的连接失败或关闭（在响应后） • 身份验证成功或失败 • 请求包含错误 • 与 AsyncOS API 进行网络配置更改通信时出现错误
合并事件日志	统一事件日志在单个日志行中汇总每个邮件事件。使用此日志类型，您可以减少发送到安全信息和事件管理 (SIEM) 供应商或应用进行分析的数据（日志信息）的字节数。这些日志采用大多数 SIEM 供应商广泛使用的通用事件格式 (CEF) 日志消息格式。
CSN 日志	CSN 日志包含有关 CSN 数据上传的详细信息。可以在跟踪级别查看 CSN 数据（邮件网关和功能使用详细信息）。
高级网络钓鱼防护日志	高级网络钓鱼防护日志包含与思科高级网络钓鱼防护云服务相关的信息。大多数信息处于“信息”或“严重”级别。

记录	说明
审核日志	审核日志记录 AAA（身份验证、授权和记帐）事件。 某些审核日志详细信息如下： • 用户 - 登录 • 用户 - 登录失败，密码不正确 • 用户 - 登录失败，用户名未知 • 用户 - 登录失败，账户到期 • 用户 - 注销 • 用户 - 锁定 • 用户 - 已激活 • 用户 - 密码更改 • 用户 - 密码重置 • 用户 - 安全设置/配置文件更改 • 用户 - 已创建 • 用户 - 已删除或修改 • 用户配置 - 用户所做的配置更改。 • 组/角色 - 删除或已修改 • 组/角色 - 权限更改 • 隔离区 - 对隔离区中的邮件执行的操作。
CSA 日志	CSA 日志包含与思科安全感知云服务相关的信息。大多数信息处于“信息”或“调试”级别。

日志类型特征

下表汇总了每种日志类型的不同特征。

Table 2: 日志类型比较

						包含								
	事务	无状态	记录为文本	记录为 **mbox** 文件	记录为二进制	定期状态信息	邮件接收信息	传送信息	单个硬退回	单个软退回	注入 **SMTP** 会话	信头日志记录	传送 **SMTP** 会话	配置信息
邮件日志	•		•			•	•	•	•	•				
qmail 格式传送日志		•			•		•	•	•					
传送日志		•			•		•	•	•					
反弹日志	•		•						•	•				
状态日志		•	•			•								
域名调试日志	•		•					•	•	•				
注入调试日志	•		•				•							
系统日志	•		•			•								
CLI 审核日志	•		•			•								
FTP 服务器日志	•		•			•								
HTTP 日志	•		•			•								
NTP 日志	•		•			•								
LDAP 日志	•		•											
反垃圾邮件日志	•		•			•								

						包含								
	事务	无状态	记录为文本	记录为 mbox 文件	记录为二进制	定期状态信息	邮件接收信息	传送信息	单个硬退回	单个软退回	注入 SMTP 会话	信头日志记录	传送 SMTP 会话	配置信息
反垃圾邮件存档				•										
灰色邮件引擎日志	•		•			•								
灰色邮件存档				•										
防病毒日志	•		•			•								
防病毒存档				•										
AMP 引擎日志	•		•			•								
AMP 存档				•										
Scaning 日志	•		•			•								
垃圾邮件隔离区	•		•			•								
垃圾邮件隔离区 GUI	•		•			•								
安全/阻止列表日志	•		•			•								
报告日志	•		•		•									
报告查询日志	•		•		•									

						包含								
	事务	无状态	记录为文本	记录为 mbox 文件	记录为二进制	定期状态信息	邮件接收信息	传送信息	单个硬退回	单个软退回	注入 SMTP 会话	信头日志记录	传送 SMTP 会话	配置信息
更新程序日志			•											
跟踪日志	•				•	•	•	•	•	•				
身份验证日志	•		•											
配置历史记录日志	•		•											
API 日志	•		•											
合并事件日志	•		•				•	•						
CSN 日志	•		•			•								•
高级网络钓鱼防护日志	•		•											
审核日志			•											

日志检索方法

可根据以下其中一个文件传输协议检索日志文件。在日志订用过程中，当使用 GUI 或 logconfig 命令创建或编辑日志订用时，可以设置协议。

Note 在某个日志上使用日志推送方法时，该日志在本地无法用于故障排除或者通过 CLI 进行搜索。

Table 3: 日志传输协议

手动下载	使用这种方法，随时可以通过在“日志订用”(Log Subscriptions) 页面单击日志目录链接，然后单击要访问的日志文件，来访问日志文件。根据使用的浏览器，可以在浏览器窗口中查看文件、打开文件，或将文件另存为文本文件。此方法使用 HTTP(S) 协议，也是默认的检索方法。 **Note** 使用此方法无法检索集群中任何计算机的日志，而不管是何级别（计算机、组或集群级别），即使在 CLI 中指定此方法亦是如此。
FTP 推送	此方法可将日志文件定期推送到远程计算机上的 FTP 服务器。订用要求提供远程计算机的用户名、密码和目标目录。日志文件将根据您设置的回滚计划进行传输。
SCP 推送	此方法可将日志文件定期推送到远程计算机上的 SCP 服务器。此方法要求在远程计算机上存在使用 SSH1 或 SSH2 协议的 SSH SCP 服务器。订用要求提供远程计算机的用户名、密码和目标目录。日志文件将根据您设置的回滚计划进行传输。

Syslog Push	此方法会将日志消息发送到远程系统日志服务器。此方法符合 RFC 3164 标准。 **Note** 只有基于文本的日志可以使用系统日志推送进行传输。 选择系统日志推送方法后，在下列字段中输入以下信息： 1. **主机名 (Hostname)** – 输入远程系统日志服务器的主机名。 2. **端口 (Port)** – 输入远程系统日志服务器的端口号。 **Note** 默认使用的端口号为 514。 3. **协议 (Protocol)** - 选择所需的协议（UDP 或 TCP）进行日志传输。 4. **邮件最大大小 (Maximum message size)** - 输入要发送到远程系统日志服务器的日志邮件的最大大小（以字节为单位）。 **Note** [对于 TCP 协议]邮件最大大小值必须是一个介于 1024 和 65535 字节之间的整数。 **Note** [对于 UDP 协议]邮件最大大小值必须是一个介于 1024 和 9216 字节之间的整数。 5. **设备 (Facility)** - 如果需要，为日志选择所需的设备。 **Note** 默认情况下，在下拉列表中选择“身份验证(Auth)”设备选项。 6. **TLS** - [仅适用于 TCP 协议]：选择此选项可通过 TLS 连接将日志消息从邮件网关发送到远程系统日志服务器。 **Note** 如果选择 TLS 选项，请确保在邮件网关中添加有效的客户端证书，以便在邮件网关和远程系统日志服务器之间建立 TLS 连接。 **Note** 系统日志推送方法使用在邮件网关的“SSL 配置 (SSL Configuration)”页面的“其他 TLS 客户端服务 (Other TLS Client Services)”选项中选择的相同 TLS 版本。 **Note** 系统日志推送方法的 TLS 支持会使用 DEFAULT SSL 密码列表。DEFAULT 关键字是 OpenSSL DEFAULT 密码字符串，通常为 `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`。
[仅适用于统一事件日志] AWS S3 推送	此方法会定期将日志文件推送到 Amazon Web 服务 (AWS) 公有云上提供的 Amazon 简单存储服务 (S3) 存储桶。订用需要 S3 存储桶名称、访问密钥和密钥来访问 Amazon S3 存储桶。您可以设置滚动更新计划以传输日志文件。 **Note** 请确保您拥有有效的 AWS S3 存储桶以使用此检索方法。有关详细信息，请参考以下网址上提供的 AWS 用户文档：https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html。

日志文件名和目录结构

AsyncOS 会根据日志订用名称为每个日志订用创建目录。日志文件在目录中的实际名称由指定的日志文件名、启动日志文件的时间戳以及单字符状态代码组成。可使用以下公式创建日志文件名：

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

状态代码可以是 .current 或 .s（表示已保存）。只能传送或删除已保存状态的日志文件。

日志回滚和传输计划

日志文件由日志订用创建，并根据满足的第一个用户指定的条件进行回滚（并调用，如选择基于推送的检索选项）：最大文件大小或计划回滚。在 CLI 中使用 logconfig 命令，或在 GUI 中使用“日志订用”页面配置最大文件大小和计划回滚的时间间隔。此外，还可以在 GUI 中使用**立即回滚**按钮，或在 CLI 中使用 rollovernow 命令对选定的日志订用进行回滚。有关计划回滚的详细信息，请参阅滚动更新日志订用, on page 70。

设备会对使用手动下载检索的日志进行保存，直至日志达到指定的最大数量（默认为 10 个文件）或直至系统需要更多的日志文件存储空间。

默认启用的日志

邮件网关预配置了很多默认启用的日志订用（其他日志可根据您应用的许可证密钥进行配置）。默认情况下，检索方法是“手动下载”(Manually Download)。

所有预配置日志订用的日志级别均为 3，但 error_logs 日志订用除外。此类日志的级别为 1，以便其中仅包含错误。有关详细信息，请参阅日志级别, on page 67。有关创建新日志订用或修改现有日志订用的信息，请参阅日志订用, on page 66。

日志类型

日志文件中的时间戳

以下日志文件包括日志自身的开始和结束日期、AsyncOS 的版本以及 GMT 偏移（以秒为单位，且仅在日志开头显示）：

- 防病毒日志
- LDAP 日志
- 系统日志
- 邮件日志

使用文本邮件日志

这类日志包含有关邮件接收、邮件传送以及退回的详细信息。这些日志是重要的信息来源，可帮助了解特定邮件的传送情况和分析系统性能。

这些日志不需要任何特殊配置。但是，必须正确配置系统才能查看附件名称，而且不一定会记录附件名称。有关信息，请参阅启用邮件跟踪和邮件跟踪概览。

下表显示了文本邮件日志中显示的信息：

Table 4: 文本邮件日志统计信息

统计信息	说明
ICID	注入连接 ID。目标至系统的 SMTP 连接的数字标识符，通过此连接可发送 1 到上千封邮件。
DCID	传输连接 ID。目标至另一服务器的 SMTP 连接的数字标识符，每个连接可发送 1 至成千上万封邮件，且每个连接会在一次邮件传送中传送部分或全部 RID。
RCID	RPC 连接 ID。目标至垃圾邮件隔离区的 RPC 连接的数字标识符。可使用此标识符追踪发往/发自垃圾邮件隔离区的邮件。
MID	邮件 ID：使用此 ID 跟踪流经日志的邮件。
RID	收件人 ID：为每个邮件收件人分配一个 ID。
New	新连接已发起。
开始	已开始新的邮件。

解释文本邮件日志

使用以下示例作为解释日志文件的指南。

Note 日志文件中的行目没有编号。在此处对它们进行编号仅用于示例演示。

Table 5: 文本邮件日志详细信息

1	`Mon Apr 17 19:56:22 2003 Info:`
	`New SMTP ICID 5 interface Management (10.1.1.1)`
	`address 10.1.1.209 reverse dns host remotehost.com verified yes`

2	`Mon Apr 17 19:57:20 2003 Info:` `Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info:` `MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info:` `MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info:` `MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`

7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

可参考下表来阅读上文介绍的日志文件。

Table 6: 文本邮件日志详细信息示例

行号	说明
1	发起到系统的新连接并分配注入 ID (ICID)“5”。该连接在管理 IP 接口上收到，并从地址为 10.1.1.209 的远程主机上发起。
2	客户端发出 MAIL FROM 命令后，为邮件分配邮件 ID (MID) 6。
3	识别和接受发件人地址。
4	识别收件人，并且分配收件人 ID (RID)“0”。
5	接受 MID 5，将其写入磁盘并确认。
6	接收成功，接收连接断开。
7	邮件传送过程随后开始。系统为其分配了从 192.168.42.42 到 10.5.3.25 的传输连接 ID (DCID)“8”。
8	开始到 RID“0”的邮件传送。
9	从 MID 6 到 RID“0”的传送成功。
10	传送连接断开。

文本邮件日志条目示例

以下是不同情景中的日志条目示例。

邮件注入和传送

发送给单个收件人的一封邮件注入邮件网关中。已成功传输该邮件。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
```

```
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

成功的邮件传送

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

不成功的邮件传输（硬退回）

具有两个收件人的一封邮件注入邮件网关中。传输过程中，目标主机返回5XX错误，这表示无法将邮件传输到任何一个收件人。邮件网关通知发件人，并从队列中删除这些收件人。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address
64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

成功传送后发生软退回

一封邮件注入邮件网关中。在第一次尝试传输时，邮件被软退回并且排队等候将来传输。第二次尝试时，邮件被成功传送。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23
2003

Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

scanconfig 命令的邮件扫描结果

当邮件无法分解为各个组成部分时（删除附件时），可以使用 scanconfig 命令确定系统行为。可选择的命令包括 Deliver、Bounce 以及 Drop。

下文示例展示的是 `scanconfig` 设为 Deliver 的文本邮件日志。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line
seen before first header


Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

下文示例展示的是 `scanconfig` 设为 drop 的文本邮件日志。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
```

```
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

包含附件的邮件

在本例中，条件为“邮件正文包含”的内容过滤器已配置为支持附件名称识别：

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes

Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0

Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

请注意，三个附件中的第二附件采用 Unicode 格式。在无法显示 Unicode 的终端上，这些附件以引用的可打印格式显示。

在 DANE 支持下的成功邮件传送

邮件到达单个收件人的邮件网关。邮件网关从 DNS 服务器请求安全 DNS MX 记录、DNS A 记录和 TLSA 记录。如果选择 DANE 为“强制”，TLSA 记录将根据收件人域的 x.509 证书值进行验证。如果 TLSA 记录验证成功，则邮件将传送给收件人。

```
Tue Nov 13 12:13:33 2018 Debug: Trying DANE MANDATORY for example.org
Tue Nov 13 12:13:33 2018 Debug: SECURE MX record(mail.example.org) found for example.org
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q('mail.example.org', 'CNAME')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QN('mail.example.org', 'CNAME',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QIP  ('mail.example.org','CNAME','8.8.8.8',60)
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q  ('mail.example.org', 'CNAME', '8.8.8.8')
Tue Nov 13 12:13:34 2018 Debug: DNSSEC Response data([], , 0, 1799)
Tue Nov 13 12:13:34 2018 Debug: Received NODATA for domain mail.example.org type CNAME
Tue Nov 13 12:13:34 2018 Debug: No CNAME record(NoError) found for domain(mail.example.org)
Tue Nov 13 12:13:34 2018 Debug: SECURE A record (4.31.198.44) found for
MX(mail.example.org) in example.org
Tue Nov 13 12:13:34 2018 Info: New SMTP DCID 92 interface 10.10.1.191 address 4.31.198.44
```

```
port 25
Tue Nov 13 12:13:34 2018 Info: ICID 13 lost
Tue Nov 13 12:13:34 2018 Info: ICID 13 close
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q('_25._tcp.mail.example.org', 'TLSA')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QN('_25._tcp.mail.example.org', 'TLSA',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QIP
('_25._tcp.mail.example.org','TLSA','8.8.8.8',60)
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q  ('_25._tcp.mail.example.org', 'TLSA', '8.8.8.8')
Tue Nov 13 12:13:35 2018 Debug: DNSSEC Response data(['0301010c72ac70b745ac19998811b13
1d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0, 1799)
Tue Nov 13 12:13:35 2018 Debug: DNS encache (_25._tcp.mail.example.org, TLSA,
[(2550119024205761L, 0,
'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
Tue Nov 13 12:13:35 2018 Debug: SECURE TLSA Record found for MX(mail.example.org) in
example.org
Tue Nov 13 12:13:36 2018 Info: DCID 92 Certificate verification successful
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384 for example.org
Tue Nov 13 12:13:36 2018 Info: Delivery start DCID 92 MID 23 to RID [0]
```

邮件传送因证书验证失败而失败

邮件到达单个收件人的邮件网关。邮件网关从 DNS 服务器请求安全 DNS MX 记录、DNS A 记录和 TLSA 记录。如果选择 DANE 为“强制”，TLSA 记录将根据收件人域的 x.509 证书值进行验证。如果证书验证失败，将在稍后传送邮件。如果找不到安全 TLSA 记录，则退回邮件。

```
Wed Nov 14 05:52:08 2018 Debug: DNS query: QN('server1.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 05:52:08 2018 Debug: DNS query: QIP
('server1.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q  ('server1.example.net', 'CNAME', '10.10.2.184')
Wed Nov 14 05:52:08 2018 Debug: DNSSEC Response data([], , 0, 284)
Wed Nov 14 05:52:08 2018 Debug: Received NODATA for domain server1.example.net type CNAME
Wed Nov 14 05:52:08 2018 Debug: No CNAME record(NoError) found for domain(server1.example.net)
Wed Nov 14 05:52:08 2018 Debug: Secure CNAME(server1.example.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: SECURE A record (10.10.1.198) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Info: New SMTP DCID 102 interface 10.10.1.191 address 10.10.1.198
 port 25
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with CNAME(server1.example.net) for
MX(someone.cs2.example.net) in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.server1.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(server1.example.net) in
example.net
Wed Nov 14 05:52:08 2018 Debug: DCID 102 All TLSA records failed for certificate not trusted
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Info: DCID 102 Certificate verification successful
Wed Nov 14 05:52:08 2018 Info: DCID 102 TLS success protocol TLSv1.2 cipher
DHE-RSA-AES128-SHA256
for example.net
Wed Nov 14 05:52:08 2018 Info: Delivery start DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: Message done DCID 102 MID 26 to RID [0]
```

```
Wed Nov 14 05:52:08 2018 Info: MID 26 RID [0] Response 'ok:  Message 31009 accepted'
Wed Nov 14 05:52:08 2018 Info: Message finished MID 26 done
```

```
Wed Nov 14 06:36:22 2018 Debug: Trying DANE MANDATORY for example.net
Wed Nov 14 06:36:22 2018 Debug: SECURE MX record(someone.cs2.example.net) found for
example.net
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('someone.cs2.example.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('someone.cs2.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP
('someone.cs2.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('someone.cs2.example.net', 'CNAME',
'10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data(['mail.example2.net.'], secure, 0,
3525)
Wed Nov 14 06:36:22 2018 Debug: DNS encache (someone.cs2.example.net, CNAME,
[(2692348132363369L, 0,
'SECURE', 'mail.example2.net')])
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('mail.example2.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('mail.example2.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP  ('mail.example2.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('mail.example2.net', 'CNAME', '10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data([], , 0, 225)
Wed Nov 14 06:36:22 2018 Debug: Received NODATA for domain mail.example2.net type CNAME
Wed Nov 14 06:36:22 2018 Debug: No CNAME record(NoError) found for domain(mail.example2.net)
Wed Nov 14 06:36:22 2018 Debug: Secure CNAME(mail.example2.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: INSECURE A record (10.10.1.197) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net) in example.net
Wed Nov 14 06:36:22 2018 Info: New SMTP DCID 104 interface 10.10.1.191 address 10.10.1.197
 port 25
Wed Nov 14 06:36:36 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 06:36:36 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:36 2018 Debug: DCID 104 All TLSA records failed for certificate not trusted
Wed Nov 14 06:36:36 2018 Info: MID 27 DCID 104 DANE failed for the domain example.net:
DANE Certificate verification failed
Wed Nov 14 06:36:36 2018 Info: Failed for all MX hosts in example.net
```

邮件传送因 TLSA 记录无效而失败

邮件到达单个收件人的邮件网关。邮件网关从 DNS 服务器请求安全 DNS MX 记录、DNS A 记录和 TLSA 记录。如果选择 DANE 为“强制”，TLSA 记录将根据收件人域的 x.509 证书值进行验证。如果找到无效的 TLSA 记录，稍后将尝试发送邮件，否则会退回邮件。

```
Tue Aug 7 05:15:18 2018 Debug: Trying DANE MANDATORY for example-dane.net
Tue Aug 7 05:15:18 2018 Debug: SECURE MX record (someone.example-dane.net) found for
test-tlsabogus.net
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('someone.example-dane.net', 'CNAME',
'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
('someone.example-dane.net','CNAME','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME',
'10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data ([], , 0, 300)
Tue Aug 7 05:15:18 2018 Debug: SECURE A record (10.10.1.198) found for MX
(someone.example-dane.net)
in example-dane.net
```

```
Tue Aug 7 05:15:18 2018 Info: ICID 32 close
Tue Aug 7 05:15:18 2018 Info: New SMTP DCID 61 interface 10.10.1.194 address 10.10.1.198
port 25
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('_25._tcp.someone.example-dane.net', 'TLSA',

'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
('_25._tcp.someone.example-dane.net','TLSA','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA',
'10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data
(['03010160b3f16867357cdfef37bb6acd687af54f
225e3bfa945e1d37bfd37bd4eb6020'], bogus, 0, 60)
Tue Aug 7 05:15:18 2018 Debug: DNS encache (_25._tcp.someone.example-dane.net, TLSA,
[(11065394975822091L,
 0, 'BOGUS', '03010160b3f16867357cdfef37bb6acd687af54f225e3bfa945e1d37bfd37bd4eb6020')])
Tue Aug 7 05:15:18 2018 Debug: BOGUS TLSA Record is found for MX (someone.example-dane.net)

in example-dane.net
Tue Aug 7 05:15:18 2018 Debug: Trying next MX record in example-dane.net
Tue Aug 7 05:15:18 2018 Info: MID 44 DCID 61 DANE failed: TLSA record BOGUS
Tue Aug 7 05:15:18 2018 Debug: Failed for all MX hosts in example-dane.net
```

因找不到 **TLSA** 记录而退回至伺机 **TLS**

邮件到达单个收件人的邮件网关。邮件网关从 DNS 服务器请求安全 DNS MX 记录、DNS A 记录和 TLSA 记录。如果您选择 DANE 为“伺机”，则 TLSA 记录将根据收件人域的 x.509 证书值进行验证。如果找不到收件人域的 TLSA 记录，则使用伺机 TLS 来加密 SMTP 会话。

```
Wed Sep 12 06:51:32 2018 Debug: Trying DANE OPPORTUNISTIC for example-dane.com
Wed Sep 12 06:51:32 2018 Debug: SECURE MX record (mx.example-dane.com) found for
digitalhellion.com
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QN ('mx.example-dane.com', 'CNAME',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QIP ('mx.example-dane.com', 'CNAME','8.8.8.8',60)
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME', '8.8.8.8')
Wed Sep 12 06:51:32 2018 Debug: DNSSEC Response data ([], , 0, 1799)
Wed Sep 12 06:51:32 2018 Debug: Received NODATA for domain mx.example-dane.com type CNAME
Wed Sep 12 06:51:32 2018 Debug: No CNAME record (NoError) found for domain
(mx.example-dane.com)
Wed Sep 12 06:51:32 2018 Debug: SECURE A record (162.213.199.115) found for MX
(mx.example-dane.com)
in example-dane.com
Wed Sep 12 06:51:32 2018 Info: ICID 1 lost
Wed Sep 12 06:51:32 2018 Info: ICID 1 close
Wed Sep 12 06:51:33 2018 Info: New SMTP DCID 2 interface 10.10.1.173 address 162.213.199.115
 port 25
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QN ('_25._tcp.mx.example-dane.com', 'TLSA',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QIP
('_25._tcp.mx.example-dane.com','TLSA','8.8.8.8', 60)
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA',
'8.8.8.8')
Wed Sep 12 06:51:34 2018 Debug: DNSSEC Response data ([], , 3, 1798)
Wed Sep 12 06:51:34 2018 Debug: Received NXDomain for domain _25._tcp.mx.example-dane.com'
 type TLSA
Wed Sep 12 06:51:34 2018 Debug: No TLSA record (NXDomain) found for MX (mx.example-dane.com)
Wed Sep 12 06:51:34 2018 Debug: Falling back to conventional TLS for MX (mx.example-dane.com)

in example-dane.com
```

```
Wed Sep 12 06:51:34 2018 Info: MID 1 DCID 2 DANE failed for the domain example-dane.com:
No TLSA Record
Wed Sep 12 06:51:34 2018 Info: DCID 2 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384
Wed Sep 12 06:51:35 2018 Info: Delivery start DCID 2 MID 1 to RID [0]
```

根据发件人的来源国家/地区收到的邮件

在本示例中，日志显示根据特定发件人组的源国家/地区接收的邮件。

```
Thu Apr  6 06:50:18 2017 Info: ICID 73 ACCEPT SG ALLOWED_LIST match country[us] SBRS -10.0
 country United States
```

邮件附件中的最大 URL 数超过 URL 扫描限制

在本示例中，日志显示邮件附件中的 URL 数超过 URL 扫描限制

```
Wed Nov 8 13:35:48 2017 Info:  MID $mid not completely scanned for URL Filtering. Error:
$error
```

邮件正文中的最大 URL 数超过 URL 扫描限制

在本示例中，日志显示邮件正文中的 URL 数超出了 URL 扫描限制。

```
Wed Nov 8 13:37:42 2017 Info: MID 976 not completely scanned for URL Filtering.
Error: The number of URLs in the message body exceeded the URL scan limit.
```

缩短的恶意 URL 重定向到思科代理服务器

在本示例中，日志显示一个因信誉得分为 -3 而标记为恶意的缩短 URI，并重定向到思科安全代理服务器。

```
Tue Nov 7 10:42:41 2017 Info: MID 9 having URL: http://ow.ly/Sb6O30fJvVn has been expanded
 to http://bit.ly/2frAl1x
Tue Nov 7 10:42:42 2017 Info: MID 9 having URL: http://bit.ly/2frAl1x has been expanded to
 http://thebest01.wayisbetter.cn/?cMFN
Tue Nov 7 10:42:42 2017 Info: MID 9 URL http://thebest01.wayisbetter.cn/?cMFN has reputation
 -3.854 matched Action: URL redirected to Cisco Security proxy
Tue Nov 7 10:42:42 2017 Info: MID 9 rewritten to MID 10 by
url-reputation-proxy-redirect-action filter 'aa'
```

无法在邮件中扩展缩短的 URL

在本示例中，日志显示邮件中的缩短 URL 无法扩展到实际的 URL。

```
Mon Oct 30 10:58:59 2017 Info: MID 36 having URL: http://ow.ly/P0Kw30fVst3 has been expanded
 to http://bit.ly/2ymYWPR
Mon Oct 30 10:59:00 2017 Info: MID 36 having URL: http://bit.ly/2ymYWPR has been expanded
to http://ow.ly/cTS730fVssH
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://ow.ly/cTS730fVssH has been expanded
 to http://bit.ly/2xK8PD9
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://bit.ly/2xK8PD9 has been expanded
to http://ow.ly/lWOi30fVssl
Mon Oct 30 10:59:02 2017 Info: MID 36 having URL: http://ow.ly/lWOi30fVssl has been expanded
 to http://bit.ly/2ggHv9e
Mon Oct 30 10:59:03 2017 Info: MID 36 having URL: http://bit.ly/2ggHv9e has been expanded
to http://ow.ly/4fSO30fVsqx
Mon Oct 30 10:59:04 2017 Info: MID 36 having URL: http://ow.ly/4fSO30fVsqx has been expanded
 to http://bit.ly/2hKEFcW
```

```
Mon Oct 30 10:59:05 2017 Info: MID 36 having URL: http://bit.ly/2hKEFcW has been expanded
to http://ow.ly/NyH830fVsq6
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://ow.ly/NyH830fVsq6 has been expanded
 to http://bit.ly/2ysnsNi
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://bit.ly/2ysnsNi has been expanded
to http://ow.ly/JhUN30fVsnL
Mon Oct 30 10:59:07 2017 Info: MID 36 having URL: http://ow.ly/JhUN30fVsnL has been expanded
 to http://bit.ly/2hKQmAe
Mon Oct 30 10:59:07 2017 Info: MID 36 URL http://bit.ly/2hKQmAe is marked malicious due to
 : URL depth exceeded
Mon Oct 30 11:04:48 2017 Warning: MID 40 Failed to expand URL http://mail1.example.com/abcd
 Reason: Error while trying to retrieve expanded URL
Mon Oct 30 11:04:48 2017 Info: MID 40 not completely scanned for URL Filtering. Error:
Message has a shortened URL that could not be expanded
```

邮件附件中恶意 URL 的日志条目

在本示例中，日志显示了信誉得分为 -9.5 的恶意邮件附件中的 URL。

```
Mon Nov 6 06:50:18 2017 Info: MID 935 Attachment file_1.txt URL http://jrsjvysq.net has
reputation -9.5 matched
Condition: URL Reputation Rule
```

由于提取失败而标记为不可扫描的邮件

在本示例中，日志显示由于附件提取失败而未被内容扫描程序扫描的邮件。

```
Tue Oct 24 08:28:58 2017 Info: Start MID 811 ICID 10
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 From: <sender@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 RID 0 To: <recipient@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 Message-ID '<example@cisco.com>'
Tue Oct 24 08:28:58 2017 Info: MID 811 Subject 'Test mail'
Tue Oct 24 08:28:58 2017 Info: MID 811 ready 5242827 bytes from <user2@sender.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Oct 24 08:28:59 2017 Info: MID 811 attachment 'gzip.tar.gz'
Tue Oct 24 08:28:59 2017 Info: MID 811 was marked as unscannable due to extraction failures.
 Reason: Error in extraction process - Decoding Errors.
Tue Oct 24 08:28:59 2017 Info: ICID 10 close
Tue Oct 24 08:28:59 2017 Info: MID 811 quarantined to "Policy" (Unscannable: due to Extraction
 Failure)
Tue Oct 24 08:28:59 2017 Info: Message finished MID 811 done
```

由于 RFC 违规而标记为不可扫描的邮件

在本示例中，日志显示了由于 RFC 违规而未被内容扫描程序扫描的邮件。

```
Tue Oct 24 08:23:26 2017 Info: Start MID 807 ICID 6
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 From: <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 RID 0 To: <recipient@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 Subject ‘Test Mail'
Tue Oct 24 08:23:26 2017 Info: MID 807 ready 427 bytes from <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Oct 24 08:23:26 2017 Info: MID 807 was marked as unscannable due to an RFC violation.
Reason: A Unix-From header was found in the middle of a header block.
Tue Oct 24 08:23:26 2017 Info: MID 807 queued for delivery
Tue Oct 24 08:23:26 2017 Info: ICID 6 close
```

生成或重写邮件的日志条目

某些功能可创建新的邮件，如重写/重定向操作（alt-rcpt-to 过滤器、反垃圾邮件 rcpt 重写、bcc() 操作、防病毒重定向等）。浏览日志时，您可能需要检查结果，添加更多 MID 以及 DCID。条目可能如下所示：

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

或者：

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

注意一点，“重写”条目可能会出现在表示使用新 MID 的日志行的后面。

发送到垃圾邮件隔离区的邮件

在用户将邮件发送到隔离区时，邮件日志会跟踪进出隔离区的移动，使用 RCID（RPC 连接 ID）标识 RPC 连接。在以下邮件日志中，邮件被标记为垃圾邮件，并发送到垃圾邮件隔离区：

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local
IronPort Spam Quarantine


Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877

Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877

Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

外部威胁源邮件日志示例

邮件日志包含有关在传入邮件中检测到的威胁以及对此类邮件执行的操作的信息。大多数信息处于“信息”或“调试”级别。

```
Thu Jun 7 20:48:10 2018 Info: MID 91 Threat feeds source 'S1' detected malicious URL:
'http://digimobil.mobi/' in attachment(s): malurl.txt. Action: Attachment stripped
```

SDR 过滤日志条目的示例

SDR 过滤信息将发布到邮件日志。大多数信息处于“信息”或“调试”级别。

- 发件人域信誉身份验证失败
- 发件人域信誉请求超时
- 发件人域信誉无效主机
- 发件人域信誉常规错误

发件人域信誉身份验证失败

在本示例中，日志显示了由于在连接到 SDR 服务时出现身份验证失败而未根据 SDR 过滤的邮件。

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>' Mon
 Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Authentication failure.
```

解决方案

在 CLI 中使用 `sdradvancedconfig` 命令配置将邮件网关连接到 SDR 服务时所需的参数。

发件人域信誉请求超时

在本示例中，日志显示了由于与 SDR 服务通信时出现请求超时错误而未根据 SDR 过滤的邮件。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Request timed out.
```

解决方案

当 SDR 请求超时时，邮件会被标记为不可扫描，并且配置的操作将应用于邮件。

发件人域信誉无效主机

在本示例中，日志显示了由于在邮件网关上配置了无效的SDR服务主机而未根据SDR过滤的邮件。

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>' Mon
 Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Invalid host configured.
```

解决方案

在 CLI 中使用 `sdradvancedconfig` 命令配置将邮件网关连接到 SDR 服务时所需的参数。

发件人域信誉常规错误

在本示例中，日志显示了由于未知错误而未根据 SDR 过滤的邮件。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Unknown error.
```

解决方案

发生未知错误时，邮件会被标记为不可扫描，并且配置的操作会应用于邮件。

思科高级网络钓鱼防护云服务已过期

在本例中，日志显示了思科高级网络钓鱼防护云服务将到期。

```
Wed May 6 11:47:45 2020 Critical: The Cisco Advanced
Phishing Protection Cloud Service has expired and is disabled. Contact
your Cisco Account Manager to renew the service and enable it.
```

解决方案：您需要联系思科客户经理续订服务并将其启用。

思科高级网络钓鱼防护云服务过期日期提醒

在本例中，日志显示了思科高级网络钓鱼防护云服务将在特定日期到期。

```
 Fri May 8 04:50:26 2020 Info: Cisco Advanced
Phishing Protection Cloud Service expires on
2020-05-10 07:00:00. You need to contact your Cisco Account
Manager to renew the service
```

解决方案：您需要联系思科客户经理以续订服务。

无 API 访问 UID 和 API 访问密钥

在本示例中，日志显示邮件网关无法轮询思科高级网络钓鱼防护云服务的到期日期，因为没有 API 访问 UID 和 API 访问密钥。

```
 Wed May 6 17:52:52 2020 Critical: Failed to poll
for the Cisco Advanced Phishing Protection Cloud Service
expiry date. You need to add the API Access UID and API Access
secret key.
```

解决方案：您需要添加 API 访问 UID 和 API 访问密钥。

API 访问 UID 或 API 访问密钥无效

在本示例中，日志显示邮件网关无法轮询思科高级网络钓鱼防护云服务的到期日期，因为 API 访问 UID 和 API 访问密钥无效。

```
Wed May 6 17:52:52 2020 Critical: Failed to poll
for the Cisco Advanced Phishing Protection Cloud Service
expiry date because the API Access Key is invalid. You need
to re-configure the API Access UID and secret key
```

解决方案：您需要重新配置 API 访问 UID 和密钥。

使用传送日志

传送日志记录有关 AsyncOS 邮件传送操作的重要信息。日志消息为“无状态”消息，这意味着所有相关信息都会逐条记录在每条日志消息中，用户无需参考上一条日志消息即可了解当前传送尝试的相关信息。

传送日志记录有关每个收件人的邮件传送操作的所有信息。所有信息以符合逻辑的方式布置，并且使用思科提供的实用程序进行转换后，可供人类进行阅读。转换工具位置：https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools

传送日志以二进制格式记录和传输，以提高资源效率。下表展示传送日志记录的信息：

Table 7: 传送日志统计信息

统计信息	说明
传送状态	成功（邮件成功传送）或退回（邮件被硬退回）
Del_time	传送时间
Inj_time	Injection time. del_time - inj_time = 收件人邮件在队列中停留的时间
字节数	消息大小
中	消息 ID
Ip	收件人主机 IP。接收或退回收件人邮件的主机的 日IP 地址
发件人	信封发件人，也称为 MAIL FROM
Source_ip	源主机 IP。传入邮件的主机的 IP 地址
代码	来自收件人主机的 SMTP 响应代码
应答	来自收件人主机的 SMTP 响应消息

统计信息	说明
Rcpt Rid	收件人 ID。收件人 ID 以 <0> 开头，有多个收件人的邮件包含多个收件人 ID
收件人	信封收件人
尝试次数	传送尝试的次数

如果传送状态为退回，传送日志中会显示以下附加信息：

Table 8: 传送日志退回信息

统计信息	说明
原因	传送过程中，SMTP 响应的 RFC 1893 增强邮件状态代码解释
代码	来自收件人主机的 SMTP 响应代码
错误	来自收件人主机的 SMTP 响应消息

如已设置日志信头（请参阅日志记录邮件信头, on page 69），传送信息后面会显示信头信息：

Table 9: 传送日志信头信息

统计信息	说明
Customer_data	标记所记录信头的开始部分的 XML 标签
信头名称	信头的名称
值	已记录信头的内容

传送日志条目示例

下文示例展示的是各种类型的传送日志条目。

成功的邮件传送

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

传送状态退回

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05 08:28:32.929 2003"

bytes="4074" mid="94157762" ip="0.0.0.0" from="campaign1@yourdomain.com"
```

```
source_ip="192.168.102.1 "reason="5.1.0 - Unknown address error" code="550"

error="["Requested action not taken: mailbox unavailable"]">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

包含日志信头的传送日志条目

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28 15:55:17.696 2003"
bytes="139" mid="202" ip="10.1.1.13" from="campaign1@yourdomain.com" source_ip="192.168.102.1"
 code="250" reply="sent">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

使用退回日志

退回日志记录有关每个退回收件人的所有信息。下表展示退回日志记录的信息：

Table 10: 退回日志统计信息

统计信息	说明
时间戳	退回事件发生的时间
日志级别	此退回日志的明细级别
退回类型	退回或延迟（例如，硬退回或软退回）
MID/RID	邮件 ID 和收件人 ID
发件人	信封发件人
收件人	信封收件人
原因	传送过程中，SMTP 响应的 RFC 1893 增强邮件状态代码解释
解决方案	来自收件人主机的 SMTP 响应代码和消息

此外，如已指定要记录的邮件大小或已设置**日志信头**（请参阅日志记录邮件信头, on page 69），退回信息后面会显示邮件和信头信息：

Table 11: 退回日志信头信息

信头	信头名称和内容
消息	所记录的邮件正文

退回日志条目示例

软退回收件人（退回类型 = 延迟）

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>


Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

硬退回收件人（退回类型 = 退回）

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0 From:<campaign1@yourdomain.com>
To:<user2@sampledomain.com>


Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no such active
account.'])"
```

包含邮件正文和日志信头的退回日志

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0 From:<campaign1@yourdomain.com>
To:<user@sampledomain.com>


Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers: ['xname:
userID2333']' Message: Message-Id:



<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

Note 文本字符串 \015\012 表示换行（例如 CRLF）。

使用状态日志

状态日志记录 CLI 状态命令中的系统统计信息，包括 status、status detail 以及 dnsstatus 命令。记录期限使用 logconfig 中的 setup 子命令设置。状态日志中的每个计数器或记录的速率为从上次重置计数器起至当前的值。

了解状态日志

下表展示状态日志标签和匹配的系统统计信息。

Table 12: 状态日志统计信息

统计信息	说明
CPULd	CPU Utilization
DskIO	磁盘 I/O 利用率
RAMUtil	内存使用率
QKUsd	已用队列容量 (KB)
QKFre	可用队列容量 (KB)
CrtMID	邮件ID(MID)
CrtICID	注入连接 ID (ICID)
CRTDCID	传送连接 ID (DCID)
InjBytes	已注入的总邮件大小（字节）
InjMsg	注入的邮件数量
InjRcp	注入的收件人数量
GenBncRcp	生成的退回收件人数量
RejRcp	拒绝的收件人数量
DrpMsg	丢弃的邮件数量
SftBncEvnt	软退回事件的数量
CmpRcp	已经完成的收件人数量
HrdBncRcp	硬退回的收件人数量
DnsHrdBnc	DNS 硬退回
5XXHrdBnc	5XX 硬退回
FltrHrdBnc	内容过滤的硬退回
ExpHrdBnc	过期的硬退回
OtrHrdBnc	其他硬退回
DlvRcp	传送的收件人数量

统计信息	说明
DelRcp	已删除的收件人
GlbUnsbHt	全局取消订用命中数
ActvRcp	正在处理的收件人
UnatmptRcp	未尝试发送的收件人
AtmptRcp	已经尝试发送的收件人
CrtCncIn	当前的入站连接数
CrtCncOut	当前的出站连接数
DnsReq	DNS 请求
NetReq	网络请求数
CchHit	缓存命中数
CchMis	缓存丢失数
CchEct	缓存排斥数
CchExp	缓存过期
CPUTTm	应用的 CPU 使用总时间
CPUETm	应用启动后经过的时间
MaxIO	邮件进程的每秒最大磁盘 I/O 操作数
RamUsd	分配的内存（用字节表示）
SwIn	换入的内存。
SwOut	换出的内存。
SwPgIn	页入的内存。
SwPgOut	页出的内存。
MMLen	系统中的邮件总数
DstInMem	内存中的目标对象数量
ResCon	资源节省 tarpit 值。由于系统负载繁重，传入邮件接受按此秒数延迟
WorkQ	此为工作队列中的当前邮件数

统计信息	说明
QuarMsgs	策略、病毒或爆发隔离区中的邮件数量（出现在多个隔离区的邮件只计算一次）
QuarQKUsd	策略、病毒和爆发隔离区邮件使用的千字节数
LogUsd	日志分区的使用百分比
SophLd	Sophos 防病毒扫描的 CPU 使用百分比
McafLd	McAfee 防病毒扫描的 CPU 使用百分比
CASELd	CASE 扫描的 CPU 使用百分比
TotalLd	CPU 消耗总量
LogAvail	可用于日志文件的磁盘空间大小
EuQ	垃圾邮件隔离区中邮件的估计数量
EuqRls	垃圾邮件隔离区放行队列中邮件的估计数量
RptLD	报告过程中的 CPU 负载
QtnLd	隔离过程中的 CPU 负载
EncrQ	加密队列中的邮件

状态日志示例

```
Fri Feb 28 12:11:48 2020 Info: Status: CPULd 45 DskIO 22 RAMUtil 22 QKUsd 6676975
QKFre 1711633 CrtMID 6130195 CrtICID 722770 CrtDCID 54 InjMsg 4572789 InjRcp
4575323 GenBncRcp 255536 RejRcp 20388 DrpMsg 469642 SftBncEvnt 0 CmpRcp 3650806 HrdBncRcp
255536
DnsHrdBnc 23 5XXHrdBnc 28 FltrHrdBnc 255485 ExpHrdBnc 0
OtrHrdBnc 0 DlvRcp 3394965 DelRcp 305 GlbUnsbHt 0 ActvRcp 65 UnatmptRcp 65 AtmptRcp 0
CrtCncIn 9
CrtCncOut 0 DnsReq 7756744 NetReq 7769130 CchHit 8373490 CchMis
1989637 CchEct 1625236 CchExp 1569329 CPUTTm 37 CPUETm 62 MaxIO 465600 RAMUsd 1473355956
MMLen 54782
DstInMem 11 ResCon 0 WorkQ 54710 QuarMsgs 375
QuarQKUsd 145096 LogUsd 26 SophLd 15 BMLd 0 CASELd 0 TotalLd 100 LogAvail 116G EuQ 64 EuqRls
 0 CmrkLd 0
McafLd 9 SwIn 122 SwOut 5295 SwPgIn 368 SwPg Out 63639
SwapUsage 4% RptLd 0 QtnLd 19 EncrQ 0 InjBytes 516664777890
```

使用域调试日志

域调试日志记录邮件网关与指定收件人主机之间的 SMTP 会话期间的客户端和服务器通信。此日志类型主要用来调试特定收件人主机存在的问题。

Table 13: 域调试日志统计信息

统计信息	说明
时间戳	退回事件发生的时间
日志级别	此退回日志的明细级别
发件人	信封发件人
收件人	信封收件人
原因	传送过程中，SMTP 响应的 RFC 1893 增强邮件状态代码解释
解决方案	来自收件人主机的 SMTP 响应代码和消息

域调试日志示例

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END WITH "." ON A
LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

使用注入调试日志

注入调试日志记录邮件网关与连接到系统的指定主机之间的 SMTP 会话。注入调试日志对于排除邮件网关与从互联网发起连接的客户端之间的通信问题很有帮助。该日志记录在两个系统之间传输的所有字节，并将它们分类为“发送目标”连接主机或“接收来源”连接主机。

必须通过指定 IP 地址、IP 范围、主机名或部分主机名，表明要记录的主机对话。日志将记录 IP 范围内的所有连接 IP 地址。而且，在一个部分域内的所有主机都将被记录。系统将在连接的 IP 地址上执行反向 DNS 查找，将 IP 地址转换为主机名。在 DNS 中没有相应 PTR 记录的 IP 地址不存在匹配的主机名。

此外，还必须指定要记录的会话数。

“注入调试”日志的每一行均包含下表中的如下信息。

Table 14: 注入调试日志统计信息

统计信息	说明
时间戳	数据的传输时间

统计信息	说明
ICID	注入连接 ID 是可与其他日志订用中同一连接关联的唯一标识符
发送数据/接收数据	标有“发送目标”的行是已发送到连接主机的实际字节。标有“接收来源”的行是从连接主机接收的实际字符
IP 地址	所连接主机的 IP 地址

注入调试日志示例

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220 postman.example.com
ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'
Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go ahead\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject: Test
Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the content of the
message'
Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'
```

使用系统日志

Table 15: 系统日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	记录的事件

系统日志分析

在本示例中，系统日志展示了一些提交条目，包括发出提交命令的用户的名称和用户输入的注释。

```
Wed Sep 8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:02:45 2004 Info: System is coming up

Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password

Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW

Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples

Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

使用 CLI 审核日志

***Table 16: CLI* 审核日志统计信息**

统计信息	说明
时间戳	数据的传输时间
PID	输入命令的特定 CLI 会话的进程 ID
消息	消息包含输入的 CLI 命令、CLI 输出（包括菜单、列表等）和显示的提示

CLI 审核日志示例

在本例中，CLI 审核日志显示用户对 PID 16434 输入以下 CLI 命令：who、textconfig。

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '


Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n======== ========== =========
=========== ====\nadmin Wed 11AM 3m 45s 10.1.3.14 tail\nadmin 02:32PM
0s 10.1.3.14 cli\nmail3.example.com> '


Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

使用 FTP 服务器日志

Table 17: FTP 服务器日志统计信息

统计信息	说明
时间戳	数据的传输时间
ID	连接 ID。每个 FTP 连接的单独 ID
消息	日志条目的消息部分可以是日志文件状态信息或 FTP 连接信息（登录、上传、下载、注销等）

FTP 服务器日志示例

在本例中，FTP 服务器日志记录了连接（ID：1）。显示了传入连接的 IP 地址以及活动（上传和下载文件）和注销。

```
Wed Sep 8 18:03:06 2004 Info: Begin Logfile

Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21

Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes

Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

使用 HTTP 日志

Table 18: HTTP 日志统计信息

统计信息	说明
时间戳	数据的传输时间
ID	会话 ID
req	连接计算机的 IP 地址
用户	连接用户的用户名

统计信息	说明
消息	有关所执行操作的信息。可能包括 GET 或 POST 命令，或系统状态等。

HTTP 日志示例

在本示例中，HTTP 日志展示了管理员用户与 GUI 的交互（运行“系统设置向导”[System Setup Wizard] 等）。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443

Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303

Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200

Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=19
0 HTTP/1.1 200

Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

使用 NTP 日志

Table 19: NTP 日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	消息包含目标到服务器的简单网络时间协议 (SNTP) 查询或 adjust: 消息

NTP 日志示例

在本例中，NTP 日志显示了两次轮询 NTP 主机的邮件网关。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652

Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
```

```
Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152

Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

使用扫描日志

扫描日志包含邮件网关扫描引擎的所有LOG和COMMON消息。可参阅“系统管理”一章中的“警报”部分，了解 COMMON 和 LOG 警报消息。

Table 20: 扫描日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	消息包含针对某一扫描引擎的应用故障、发送的警报、失败的警报或日志错误消息。

扫描日志示例

在本示例中，日志显示发送有关 Sophos 防病毒警告警报的邮件网关的历史记录。

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...' (attempt #0).


Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...'.


Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com
with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
database on this system is...".
```

使用反垃圾邮件日志

Table 21: 反垃圾邮件日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	消息包含反垃圾邮件更新检查，以及检查结果（是否需要引擎或反垃圾邮件规则更新）

反垃圾邮件日志示例

在本例中，反垃圾邮件日志显示反垃圾邮件引擎检查垃圾邮件定义更新和 CASE 更新：

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) : case-daemon: server
successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) : startup: Region profile:
Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy: Fuzzy plugin v7
successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) : uribllocal: running URI
blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config: Finished loading
configuration
```

使用灰色邮件日志

统计信息	说明
时间戳	数据的传输时间
消息	邮件包含有关灰色邮件引擎、状态、配置的信息等。

灰色邮件日志示例

```
Tue Mar 24 08:56:45 2015 Info: graymail [BASE] Logging at DEBUG level

Tue Mar 24 08:56:45 2015 Info: graymail [HANDLER] Initializing request handler

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Loaded graymail scanner library

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Created graymail scanner instance

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Debug mode disabled on graymail process

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Starting thread WorkerThread_0
```

使用防病毒日志

Table 22: 防病毒日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	消息包含防病毒更新检查，以及检查结果（是否需要引擎或病毒定义更新）

防病毒日志示例

在本例中，防病毒日志显示 Sophos 防病毒引擎检查病毒定义 (IDE) 更新和引擎本身的更新。

```
Thu Sep 9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep 9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine update needed

Thu Sep 9 14:18:04 2004 Info: Current IDE serial=2004090902. No update needed.
```

您可以将此暂时设置为调试级别，帮助诊断防病毒引擎为什么对给定邮件做出了特定判断。调试日志记录信息非常冗长，请谨慎使用。

使用 AMP 引擎日志

AMP 引擎日志包含以下内容的详细信息：

- 发送到文件信誉服务器的文件信誉查询和从文件信誉服务器收到的响应。
- 文件分析，如果文件已上传到文件分析服务器。文件分析的状态会定期记录，直到从文件分析服务器收到响应。

AMP 引擎日志条目示例

以下是基于某些方案的 AMP 引擎日志条目示例：

- 文件信誉和文件分析服务器的初始化, on page 40
- 文件信誉服务器未配置, on page 40
- 文件信誉查询的初始化, on page 40
- 从文件信誉服务器收到的文件信誉查询响应, on page 41
- 已上传文件进行分析以及文件分析过程, on page 42
- 未上传文件进行分析, on page 43
- 由于文件上传限制，跳过文件上传而不进行文件分析 , on page 43
- 由于文件分析服务器错误，跳过文件上传而不进行文件分析, on page 44
- 文件追溯判定已收到, on page 44

文件信誉和文件分析服务器的初始化

```
Wed Oct 5 15:17:31 2016 Info: File reputation service initialized successfully
Wed Oct 5 15:17:31 2016 Info: The following file type(s) can be sent for File Analysis:
Microsoft Windows / DOS Executable, Microsoft Office 97-2004 (OLE), Microsoft Office 2007+
 (Open XML), Other potentially malicious file types, Adobe Portable Document Format (PDF).
 To allow analysis of new file type(s), go to Security Services > File Reputation and
Analysis.
Wed Oct 5 15:17:31 2016 Info: File Analysis service initialized successfully
```

文件信誉服务器未配置

```
Tue Oct 4 23:15:24 2016 Warning: MID 12 reputation query failed for attachment 'Zombies.pdf'
 with error "Cloud query failed"
```

文件信誉查询的初始化

```
Fri Oct 7 09:44:04 2016 Info: File reputation query initiating. File Name = 'mod-6.exe',
MID = 5, File Size = 1673216 bytes,
```

```
File Type = application/x-dosexec
```

统计信息	说明
文件名	其 SHA-256 散列标识符发送到文件信誉服务器的文件的名称。 如果文件名不可用，则显示为“未知”。
MID	用于跟踪通过邮件管道传递的邮件的邮件 ID。
文件大小	将其 SHA-256 散列标识符发送到文件信誉服务器的文件的大小。
文件类型	将其 SHA-256 散列标识符发送到文件信誉服务器的文件的类型。 以下是支持的文件类型： • Microsoft Windows / DOS Executable • Microsoft Office 97-2004 (OLE) • Microsoft Office 2007+ (Open XML) • 其他潜在恶意文件类型 • Adobe 便携式文档格式 (PDF)

从文件信誉服务器收到的文件信誉查询响应

```
Fri Oct 7 09:44:06 2016 Info: Response received for file reputation query from Cloud. File
Name = 'mod-6.exe', MID = 5, Disposition = MALICIOUS, Malware = W32.061DEF69B5-100.SBX.TG,
Reputation Score = 73, sha256 =
061def69b5c100e9979610fa5675bd19258b19a7ff538b5c2d230b467c312f19, upload_action = 2
```

统计信息	说明
文件名	其 SHA-256 散列标识符发送到文件信誉服务器的文件的名称。 如果文件名不可用，则显示为“未知”。
MID	用于跟踪通过邮件管道传递的邮件的邮件 ID。
处理结果	文件信誉处理值为： • 恶意 • 正常 • 文件未知 - 信誉得分为零时。 • 判定未知 - 处置为“文件未知”，且值为非零时。 • 低风险 (LOW RISK) - 当文件分析后在文件中找不到动态内容时，所得判决是低风险。文件未送交文件分析，邮件将通过邮件管道传递。
恶意软件	恶意软件威胁的名称。

统计信息	说明
信誉得分	文件信誉服务器分配给文件的信誉得分。 如果文件处置是**判定未知 (VERDICT UNKNOWN)**，邮件网关将根据信誉得分和阈值调整文件信誉判定。
上传操作	文件信誉服务器推荐的对给定文件应用的上传操作值： • 0 - 无需发送上传 • 1 - 发送文件进行上传。 **Note** 当上传操作值为“1”时，邮件网关将上传该文件。 • 2 - 不发送文件进行上传 • 3 - 仅发送元数据进行上传

已上传文件进行分析以及文件分析过程

```
Wed Sep 28 11:31:58 2016 Info: File uploaded for analysis. SHA256:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Wed Sep 28 11:36:58 2016 Info: File Analysis is running for SHA:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Fri Oct 7 07:39:13 2016 Info: File Analysis complete. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Submit Timestamp:
1475825466, Update Timestamp: 1475825953, Disposition: 3 Score: 100, run_id: 194926004
Details: Analysis is completed for the File
SHA256[16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc]
Spyname:[W32.16454AFF50-100.SBX.TG]
```

统计信息	说明
SHA256	相应文件的 SHA-256 散列标识符。
提交时间戳	邮件网关将文件上传到文件分析服务器的日期和时间。
更新时间戳	文件的文件分析完成的日期和时间
处理结果	文件信誉处置值包括： • 1 - 未检测到恶意软件 • 2 - 正常 • 3 - 恶意软件
得分	文件分析服务器分配给文件的分析分数。
运行 ID	文件分析服务器为特定文件分析分配给文件的数字值 (ID)。
Details	如果在文件分析期间报告错误，则显示其他信息，否则会指示文件的最终分析已完成。

统计信息	说明
间谍软件名称	威胁的名称（如果在文件分析期间在文件中发现恶意软件）。

未上传文件进行分析

```
Wed Sep 14 12:27:52 2016 Info: File not uploaded for analysis. MID = 0 File
SHA256[a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82] file
mime[text/plain] Reason: No active/dynamic contents exists
```

统计信息	说明
MID	用于跟踪通过邮件管道传递的邮件的邮件 ID。
文件 MIME	文件的 MIME 类型。
原因	以下是即使 upload_action 设置为“1”，文件也未上传到文件分析服务器的原因值之一： • 文件已由另一个节点上传 - 文件已通过其他邮件网关上传到文件分析服务器。 • 正在进行文件分析 - 文件已被选中进行上传且上传正在进行中。 • 文件已上传到文件分析服务器 • 不是支持的文件类型 • 文件大小超出范围 - 上传文件大小超过文件分析服务器设置的阈值限制。 • 上传队列已满 • 文件分析服务器错误 • 不存在活动/动态内容 • 一般/未知错误

由于文件上传限制，跳过文件上传而不进行文件分析

```
Tue Jun 20 13:22:56 2017 Info: File analysis upload skipped. SHA256:
b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef,Timestamp[1454782976]
details[File SHA256[b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef] file
mime[application/pdf], upload priority[Low] not uploaded, re-tries[3], backoff[986]
discarding ...]
Tue Jun 20 13:22:56 2017 Critical: The attachment could not be uploaded to the
File Analysis server because the appliance exceeded the upload limit
```

统计信息	说明
SHA256	相应文件的 SHA-256 散列标识符。
时间戳	文件无法上传到文件分析服务器的日期和时间。
Details	文件分析服务器错误的详细信息。
文件 MIME	文件的 MIME 类型。

统计信息	说明
上传优先级	上传优先级值为： • 高 - 针对所有选定的文件类型，PDF 文件类型除外。 • 低 - 仅针对 PDF 文件类型
重新尝试	对给定文件执行的上传尝试次数。 **Note** 最多可以对给定文件执行三次上传尝试。
退避 (x)	邮件网关在尝试将文件上传到文件分析服务器之前需要等待的秒数 (x)。当邮件网关达到每日上传限制时会发生此情况。
关键 (原因)	无法将附件上传到文件分析服务器，因为邮件网关超出了上传限制。

由于文件分析服务器错误，跳过文件上传而不进行文件分析

```
Sat Feb 6 13:22:56 2016 Info:SHA256:
69e17e213732da0d0cbc48ae7030a4a18e0c1289f510e8b139945787f67692a5,Timestamp[1454959409]
details[Server Response HTTP code:[502]]
```

统计信息	说明
SHA256	相应文件的 SHA-256 散列标识符。
时间戳	尝试将文件上传到文件分析服务器的日期和时间。
Details	有关文件分析服务器错误的信息。

文件追溯判定已收到

```
Fri Oct 7 07:39:13 2016 Info: Retrospective verdict received. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Timestamp: 1475832815.7,
Verdict: MALICIOUS, Reputation Score: 0, Spyname: W32.16454AFF50-100.SBX.
```

统计信息	说明
SHA256	相应文件的 SHA-256 散列标识符。
时间戳	从文件分析服务器接收文件追溯判定的日期和时间。
判定	文件追溯判定值是恶意的或安全的。
信誉得分	文件信誉服务器分配给文件的信誉得分。
Spyname	威胁的名称（如果在文件分析期间在文件中发现恶意软件）。

使用垃圾邮件隔离区日志

Table 23: 垃圾邮件日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	消息包含所采取的操作（隔离邮件、从隔离区放行的邮件等）。

垃圾邮件隔离区日志示例

在本示例中，日志展示从隔离区放行到 admin@example.com 的邮件 (MID 8298624)。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

使用垃圾邮件隔离区 GUI 日志

Table 24: 垃圾邮件 *GUI* 日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	消息包含所采取的操作，包括用户身份验证等。

垃圾邮件隔离区 GUI 日志示例

在本示例中，日志显示了成功的身份验证、登录和注销：

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82

Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

使用 LDAP 调试日志

Table 25: LDAP 调试日志统计信息

统计信息	说明
时间戳	数据的传输时间
消息	LDAP 调试消息

LDAP 调试日志示例

Note 日志文件中的行目没有编号。下文出于方便对各行进行了编号

1	Thu Sep 9 12:24:56 2004 Begin Logfile
2	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
3	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
4	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
5	Thu Sep 9 12:28:08 2004 LDAP: Clearing LDAP cache
6	Thu Sep 9 13:00:09 2004 LDAP: Query '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun (sun.qa:389)
7	Thu Sep 9 13:00:09 2004 LDAP: After substitute, query is '(&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa))'
8	Thu Sep 9 13:00:09 2004 LDAP: connecting to server
9	Thu Sep 9 13:00:09 2004 LDAP: connected
10	Thu Sep 9 13:00:09 2004 LDAP: Query (&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa)) returned 1 results
11	Thu Sep 9 13:00:09 2004 LDAP: returning: [<LDAP:>]

可参考本日志阅读上文介绍的日志文件。

Table 26: LDAP 调试日志详细信息示例

行号	说明
1	日志文件已初始化。
2 3 4	侦听程序配置为使用 LDAP 进行伪装，具体使用名为“sun.masquerade”的 LDAP 查询。 侦听程序在 LDAP 服务器上查询地址 employee@routing.qa，找到匹配项，生成伪装地址 employee@mail.qa，并根据伪装配置将该地址写入邮件信头和/或源信封。
5	用户手动运行 ldapflush。
6	查询随即发送到端口 389 sun.qa。查询模板为 (&(ObjectClass={g})(mailLocalAddress={a}))。 {g} 将替换为调用过滤器中指定的组名，rcpt-to-group 或 mail-from-group 规则均可。 {a} 将替换为具体地址。
7	这便是查询在发送到 LDAP 服务器之前的样态，接下来将发生（前面介绍的）替换。
8	此时与服务器的连接并没有建立，请建立连接。
9	发送至服务器的数据。
10	结果是空正值，这表示返回了一条记录，但因为查询没有请求任何字段，因此没有要报告的数据。查询检查数据库中是否存在匹配项时，这些数据将用于组和接受查询。

使用安全列表/阻止列表日志

下表显示在安全列表/阻止列表日志中记录的统计信息。

Table 27: 安全列表/阻止列表日志统计信息

统计信息	说明
时间戳	数据的传输时间。
消息	该消息包括采取的措施，包括用户身份验证等等。

安全列表/阻止列表日志示例

在本例中，安全列表/阻止列表日志显示了邮件网关每两个小时创建一次数据库快照。它还显示了何时将发件人添加到数据库中。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC:
10800 seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.


Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.

.........................

Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

使用报告日志

下表显示在报告日志中记录的统计信息。

Table 28: 报告日志统计信息

统计信息	说明
时间戳	数据的传输时间。
消息	该消息包括采取的措施，包括用户身份验证等等。

报告日志示例

在本示例中，报告日志显示在信息日志级别设置的邮件网关。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40

Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692

Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)
```

```
Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds

Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41

Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692

Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

使用报告查询日志

下表显示在报告查询日志中记录的统计信息。

Table 29: 报告查询日志统计信息

统计信息	说明
时间戳	数据的传输时间。
消息	该消息包括采取的措施，包括用户身份验证等等。

报告查询日志示例

在本示例中，报告查询日志显示从 2007 年 8 月 29 日到 10 月 10 日期间运行每日持续邮件流量查询的邮件网关。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENT_FILTER',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_PROCESSED'] for rollup period "day" with
interval range 2007-08-29 to 2007-10-01
with key constraints

None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
```

```
0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval
range 2007-08-29 to
2007-10-01 with key constraints None sorting on
['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

使用更新程序日志

Table 30: 更新程序日志统计信息

统计信息	说明
时间戳	数据的传输时间。
消息	消息包含系统服务更新信息，AsyncOS 更新检查以及下一次更新的计划日期和时间。

更新程序日志示例

在本示例中，日志显示邮件网关使用全新 McAfee 防病毒定义进行更新。

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update 11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for mcafee

Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:12:52
2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files
```

```
Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:17:52
2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:22:52
2008
```

更新程序日志示例

在本示例中，日志显示禁用的自动更新，以及应用于 Sophos 防病毒定义的备份。

```
Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Debug: postx updates disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Trace: command session starting

Fri Mar 10 15:05:55 2017 Info: Automatic updates disabled for engine Sophos engine

Fri Mar 10 15:05:55 2017 Info: Sophos: Backup update applied successfully

Fri Mar 10 15:05:55 2017 Info: Internal SMTP system attempting to send a message to
abshastr@ironport.com
with subject ‘Automatic updates are now disabled for sophos’ attempt #0).

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “amp”

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled
```

了解跟踪日志

跟踪日志记录了有关 AsyncOS 的邮件操作的信息。此类日志消息包含在邮件日志中。

邮件网关消息跟踪组件将使用跟踪日志创建消息跟踪数据库。由于构建数据库的过程中会使用日志文件，因此跟踪日志是动态的。跟踪日志中的信息不是供人类阅读或分析的。

您还可以使用思科安全管理器邮件和网络网关查看多个邮件网关提供的跟踪信息。

使用身份验证日志

身份验证日志记录成功的用户登录和失败的登录尝试。

Table 31: 身份验证日志统计信息

统计信息	说明
时间戳	数据的传输时间。
消息	消息包含尝试登录到邮件网关的用户的用户名以及用户权限角色详细信息（例如“admin”、“operator”等），以及用户的身份验证情况。

身份验证日志示例

在本示例中，日志显示用户“admin”、“joe”以及“dan”的登录尝试。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX

Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

由于密码错误导致双因素身份验证登录失败的示例

在本示例中，日志显示由于输入的密码不正确导致双因素身份验证登录失败。

```
Thu Mar 16 05:47:47 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:48:18 2017 Info: Two-Factor RADIUS Authentication failed.

Thu Mar 16 05:48:48 2017 Info: An authentication attempt by the user **** from
21.101.210.150 failed
```

由于超时导致双因素身份验证登录失败的示例

在本示例中，日志显示由于超时而导致的双因素身份验证登录失败。

```
Thu Mar 16 05:46:04 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:46:59 2017 Info: RADIUS server example.cisco.com communication error. No
valid responses from server (timeout).

Thu Mar 16 05:46:59 2017 Info: Two-Factor Authentication RADIUS servers timed out.
Authentication could fail due to this.
```

双因素身份验证登录成功示例

在本示例中，日志显示双因素身份验证登录成功。

```
Thu Mar 16 05:49:05 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:49:05 2017 Info: Two-Factor RADIUS Authentication was successful.

Thu Mar 16 05:49:05 2017 Info: The user admin successfully logged on from 21.101.210.150
with privilege admin using an HTTPS connection.
```

使用配置历史记录日志

配置历史记录日志包括配置文件以及列出用户名的附加部分、对用户在配置中做出更改的位置的说明及用户在确认更改时输入的评论。每次用户提交更改时，都会创建一个包含更改后的配置文件的新日志。

配置历史记录日志示例

在本示例中，配置历史记录日志会显示用户（管理员）向定义允许哪些本地用户登录系统的表添加了访客用户。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<!--

XML generated by configuration change.

Change comment: added guest user

User: admin

Configuration are described as:

This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160

Version: 6.7.0-231

Serial Number: 000000000ABC-D000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time
Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
```

```
Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>
```

使用外部威胁源引擎日志

ETF 日志包含有关 ETF 引擎、状态、配置等的信息。大多数信息处于“信息”或“调试”级别。

外部威胁源引擎日志示例

```
Thu Jun 7 04:54:15 2018 Info: THREAT_FEEDS: Job failed with exception: Invalid URL or Port
 Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source: S1
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
domain: s1.co, collection: sss
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: Observables are being fetched from the source:
 S1 between 2018-06-07 04:34:13+00:00 and 2018-06-07 05:04:13.185909+00:00
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: 21 observables were fetched from the source:
S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source: S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
domain: s1.co, collection: sss
```

ETF Source Configuration Failure - Invalid Collection Name

在本示例中，日志显示由于集合名称无效，邮件网关无法从外部威胁源来源获取威胁源。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com, cause of failure: Invalid Collection name
```

解决方案

转到 Web 界面中的邮件策略 *(Mail Policies)* > 外部威胁源管理器 *(External Threat Feeds Manager)* 页面，或在 CLI 中使用 `threatfeedsconfig > sourceconfig` 子命令，并为配置的外部威胁源来源输入正确的集合名称。

ETF Source Configuration Failure - HTTP Error

在本示例中，日志显示由于 HTTP 错误，邮件网关无法从外部威胁源来源获取威胁源。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

解决方案

转到 Web 界面中的邮件策略 *(Mail Policies)* > 外部威胁源管理器 *(External Threat Feeds Manager)*页面，或在 CLI 中使用 `threatfeedsconfig > sourceconfig` 子命令，并为配置的外部威胁源来源输入正确的轮询路径或用户身份验证凭证。

ETF Source Configuration Failure - Invalid URL

在本示例中，日志显示由于 URL 无效，邮件网关无法从外部威胁源来源获取威胁源。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

解决方案

转到 Web 界面中的邮件策略 *(Mail Policies)* > 外部威胁源管理器 *(External Threat Feeds Manager)* 页面，或在 CLI 中使用 `threatfeedsconfig > sourceconfig` 子命令，并为配置的外部威胁源来源输入正确的主机名或端口号。

使用合并事件日志

在配置日志类型为“合并事件日志”的日志订用时，如果要在单个日志行输出中包含特定邮件属性，请使用“日志字段”选项。

当您将日志订用的日志类型配置为“合并事件日志”时，默认情况下会选择以下日志字段：

- ICID
- DCID
- 序列号
- MID

Note 您不能从所选日志字段列表中删除任何默认日志字段。

合并事件日志示例

在本示例中，当您将日志订用的日志类型配置为“合并事件日志”时，日志会显示选择的所有可用字段。

```
Thu Mar 18 08:04:50 2021: CEF:0|Cisco|C100V Email Security Virtual Appliance|14.0.0-657
|ESA_CONSOLIDATED_LOG_EVENT|Consolidated Log
Event|5|deviceExternalId=42127C7DDEE76852677B-F80CE8074CD3
ESAMID=1053 ESAICID=134 ESAAMPVerdict=UNKNOWN ESAASVerdict=NEGATIVE ESAAVVerdict=NEGATIVE
ESACFVerdict=MATCH endTime=Thu Mar 18 08:04:46 2021 ESADLPVerdict=NOT_EVALUATED
dvc=10.10.193.13 ESAAttachmentDetails={'test.txt': {'AMP': {'Verdict': 'FILE UNKNOWN',
'fileHash': '7f843d263304fb0516d6210e9de4fa7f01f2f623074aab6e3ee7051f7b785cfa'},
'BodyScanner':
{'fsize': 10059}}} ESAFriendlyFrom=test@esa.com ESAGMVerdict=NEGATIVE startTime=Thu Mar 18
 08:04:29 2021
deviceInboundInterface=Incomingmail deviceDirection=0 ESAMailFlowPolicy=ACCEPT
suser=test@esa.com
cs1Label=MailPolicy cs1=DEFAULT ESAMFVerdict=NOT_EVALUATED act=QUARANTINED
ESAFinalActionDetails=To POLICY
cs4Label=ExternalMsgID cs4='<20210318070601.40490.18684@mail1.example.com>' ESAMsgSize=11873
 ESAOFVerdict=POSITIVE
duser=9076@testing.com ESAHeloIP=10.11.1.2 cfp1Label=SBRSScore cfp1=None ESASDRDomainAge=27
 years 2 months 15 days
cs3Label=SDRThreatCategory cs3=N/A cs6Label=SDRRepScore cs6=Weak ESASPFVerdict={'mailfrom':
 {'result': 'None',
'sender': 'test@esa.com'}, 'helo': {'result': 'None', 'sender': 'postmaster'}, 'pra':
{'result': 'None', 'sender':
'test@esa.com'}} sourceHostName=unknown ESASenderGroup=UNKNOWNLIST sourceAddress=10.11.1.2
 msg='Testing'
```

日志字段	CEF 字段值	CEF 字段值
前缀字段		
	CEF 格式版本	示例：0
	设备供应商	示例：思科
	设备产品	示例：C100V 邮件安全虚拟设备
	设备版本	示例：13.0.0-234
	事件类 ID	示例： ESA_CONSOLIDATED_LOG_EVENT
	事件名称	示例：统一日志事件
	严重性	示例：5
GUI 字段		
序列号	deviceExternalId	示例： 42156AC79142E979C5CD-02DE66639E9C
ICID 时间戳	开始时间	示例：Mon Jul 29 11:22:22 2019
ICID	ESAICID	示例：199
监听程序名称	deviceInboundInterface（用于传入邮件）deviceOutboundInterface（用于传出邮件）	示例：Inbound 示例：Outbound
发件人 IP	sourceAddress	示例：10.10.2.75
发件人域	sourceHostName	示例： demo.cisco.com
邮件方向	deviceDirection	示例：0 0 -> 传入 1 -> 传出
邮件语言	cs5	示例： cs5Label=ESAMsgLanguage cs5=English
SBRS 得分	cfp1	示例：cfp1Label=SBRSScore, cfp1=1.1
数据 IP	dvc	示例：10.10.2.75

日志字段	CEF 字段值	CEF 字段值
邮件发件人地理位置	cs2	示例：cs2Label=GeoLocation cs2=India
发件人的邮件过大	ESAMsgTooBigFromSender	示例：true 可能的值： true/false
速率受限 IP	ESARateLimitedIP	示例：10.10.2.75
邮件策略值	cs1	示例：cs1Label=MailPolicy cs1=default
邮件流策略值	ESAMailFlowPolicy	示例：ACCEPT
发件人组名称	ESASenderGroup	示例：UNKNOWNLIST
DHA IP	ESADHASource	示例：10.10.2.75
收件人	duser	示例：demo@test.com
远程 IP/Helo 域 IP	ESAHeloIP	示例：10.10.2.75
远程主机/Helo 域	ESAHeloDomain	示例：test.com
TLS 传出连接状态	ESATLSOutConnStatus	示例：Success 可能的值： Success/Failure
TLS 传出协议	ESATLSOutProtocol	示例：TLSv1.2
TLS 传出密码	ESATLSOutCipher	示例：ECDHE-RSA-AES128-GCM-SHA256
TLS 传入连接状态	ESATLSInConnStatus	示例：Success 可能的值： Success/Failure
TLS 传入协议	ESATLSInProtocol	示例：TLSv1.2
TLS 传入密码	ESATLSInCipher	示例：ECDHE-RSA-AES128-GCM-SHA256

日志字段	CEF 字段值	CEF 字段值
DMARC 判定	ESADMARCVerdict	示例：Success 可能的值： PermFailure/TempFailure/ Reject/Success
DKIM 判定	ESADKIMVerdict	示例：Pass 可能的值： Pass/Neutral/TempError/ PermError/HardFail/None
SPF 判定	ESASPFVerdict	示例： ESASPFVerdict={'mailfrom': {'sender': 'test@cisco.com', 'result': 'SoftFail'}, 'helo': {'sender': 'postmaster', 'result': 'None'}} 可能的值： Pass/Neutral/SoftFail/Fail/ TempError/PermError
友好发件人	ESAFriendlyFrom	示例：demo@test.com
邮件发件人	suser	示例：demo@test.com
回复收件人	ESAReplyTo	示例：demo@test.com
主体	msg	示例：This is a sample subject
MID	ESAMID	示例：101
消息 ID	cs4	示例：cs1Label=ExternalMsgID cs1=20190729112221.42958.40626 @vm21esa0075.cs21
消息大小	ESAMsgSize	示例：ESAMsgSize=32199
SDR 信誉得分	cs6	示例：cs6Label= SDRRepScore cs6=Tainted
SDR 统一域有效期	ESASDRDomainAge	示例：1 year 21 days
SDR 统一威胁类别	cs3	示例：cs3Label= SDRThreatCategory cs3=mal

日志字段	CEF 字段值	CEF 字段值
邮件过滤器判定	邮件过滤器判定	示例：MATCH 可能的值： NOT EVALUATED/MATCH/NO MATCH
AS 判定	ESAASVerdict	示例：POSITIVE 可能的值： 不 已评估/负/可疑/ BULK_MAIL/SOCIAL_MAIL/MARKETING_MAIL/POSITIVE
AV 判定	ESAAVVerdict	示例：POSITIVE 可能的值： 不 EVALUATED/NEGATIVE/REPAIRED/ENCRYPTED/UNSCANNABLE/POSITIVE
AMP 判定	ESAAMPVerdict	示例：UNKNOWN 可能的值： 不 EVALUATED/CLEAN/FA_PENDING/UNKNOWN/SKIPPED/ 不可扫描 /LOW_RISK/MALICIOUS
灰色邮件判定	ESAGMVerdict	示例：POSITIVE 可能的值： 不 EVALUATED/POSITIVE/NEGATIVE
内容过滤器判定	ESACFVerdict	示例：MATCH 可能的值： NOT EVALUATED/MATCH/NO 匹配

日志字段	CEF 字段值	CEF 字段值
病毒爆发过滤器判定	ESAOFVerdict	示例：NEGATIVE 可能的值： 不 EVALUATED/POSITIVE/NEGATIVE
DLP 判定	ESADLPVerdict	示例：VIOLATION 可能的值： NOT EVALUATED/NO TRIGGER/VIOLATION/NO VIOLATION
URL 详细信息	ESAURLDetails	示例： {url1:{expanded_url:<>, category:<>, wbrs_score:<>, in_attachment:<>, Attachment_with_url:<>,},url2:{⋯}} **Note** 如果 URL 包含 255 个以上字符，则会被截断
文件详情	ESAAttachmentDetails	示例： {name1:{source: {<>hash:<>, verdicts:<>}}} **Note** 如果文件名包含 255 个以上字符，则会被截断。
邮箱自动补救详细信息	ESAMARAction	示例： {action:<>;succesful_rcpts=<>;failed_recipients=<>;filename=<>}
DCID	ESADCID	示例：199
DCID 时间戳	结束时间	示例：Mon Jul 29 09:55:07 2019
DANE 状态	ESADaneStatus	示例：success 可能的值： success/failure

日志字段	CEF 字段值	CEF 字段值
DANE 主机	ESADaneHost	示例：testdomain.com
邮件最终操作	act	示例：act=DELIVERED 可能的值： DROPPED/BOUNCED/DELIVERED - 如果邮件未被隔离。 QUARANTINED - 如果邮件已被隔离。 DQ - 如果邮件被发送到延迟隔离区。这是一种例外，而并非隔离类型。
邮件最终操作详细信息	ESAFinalActionDetails	示例： act=DROPPED ESAFinalActionDetails= By AMP act=QUARANTINED ESAFinalActionDetails=To SPAM

Note 如果所选日志字段没有任何值（例如 "DKIMVerdict"，因为以及网关上未启用 DKIM），则日志消息中不包含该日志字段。

使用 CSN 日志

CSN 日志包含有关 CSN 数据上传的详细信息。可以在跟踪级别查看 CSN 数据（邮件网关和功能使用详细信息）。

CSN 数据日志条目示例：

- 在此示例中，日志显示邮件网关无法将 CSN 数据发送到思科，因为邮件网关智能许可证未向思科智能软件管理器 (CSSM) 注册。

```
Tue Apr 7 12:52:47 2020 Warning: Device is not
registered with CSSM. Skipping upload of CSN data
```

  解决方案：确保向思科智能软件管理器 (CSSM) 注册邮件网关智能许可证。

- 在本例中，日志显示由于思科安全服务交换 (SSE) 连接错误，邮件网关无法将 CSN 数据发送到思科。

```
Thu Apr 9 13:32:46 2020 Warning: The appliance
failed to upload CSN data. reason for failure:
SSE error: HTTP Error 503: Service Unavailable
```

解决方案：确保禁用 CSN 并在邮件网关上再次启用 CSN。

使用高级网络钓鱼防护日志

高级网络钓鱼防护日志包含与思科高级网络钓鱼防护云服务相关的信息。大多数信息处于“信息”或“严重”级别。

高级网络钓鱼防护数据日志条目示例：

- 在本例中，日志显示了邮件网关无法将邮件信头转发到思科高级网络钓鱼防护云服务，因为该服务已过期。

```
Wed May 6 18:21:40 2020 Info: eaas : You cannot
forward the MID [877] Message Headers to Cisco Advanced
Phishing Protection Cloud Service as the service has
expired
```

- 在本例中，日志显示了思科高级网络钓鱼防护云服务已过期，并已在邮件网关中禁用。

```
Wed May 6 18:21:40 2020 Info: eaas : Cisco
Advanced Phishing Protection Cloud Service has expired
and is disabled. Contact your Cisco Account manager to
renew the service and then enable it.
```

解决方案：请联系您的思科客户经理续订服务，然后将其启用。

- 在本例中，日志显示了思科高级网络钓鱼防护云服务将在特定日期到期。

```
Fri May 8 04:50:26 2020 Info: eaas : Cisco
Advanced Phishing Protection Cloud Service expires on
2020-05-10 07:00:00. You need to contact your Cisco Account
manager to renew the service.
```

解决方案：联系思科客户经理以续订服务。

使用审核日志

审核日志记录 AAA（身份验证、授权和记帐）事件。大多数信息处于“调试”或“跟踪”级别。

审核日志条目示例：

- 在本例中，日志显示了用户（例如 admin）何时：
  - 登录邮件网关的 Web 界面。
  - 从邮件网关的 Web 界面注销。

```
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,

Event: Successful login
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session established
 successfully
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: User logged out
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session terminated
```

- 在本例中，日志显示用户（例如 admin）输入了 `logconfig` CLI 命令。

```
Thu Oct  8 13:33:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User input was 'logconfig'
Thu Oct  8 13:33:46 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User input was 'Enter'
```

- 在本例中，日志显示用户（例如 admin）查看了邮件网关的旧 Web 界面上的 GUI 页面。

```
Thu Oct  8 13:35:07 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /network/dns, Event: User visited the web page.
Thu Oct  8 13:35:13 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/sslconfig, Event: User visited
 the web page.
Thu Oct  8 13:35:24 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /monitor/mail_reports/threatfeeds_report, Event: User
 visited the web page.
```

- 在本例中，日志显示使用Web界面将新用户（例如admin）添加到了邮件网关，但未提交更改。

```
Thu Oct  8 13:36:30 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Added
user "admin" and changes
will reflect after commit.
Thu Oct  8 13:37:22 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Deleted
user "admin" and changes
will reflect after commit.
```

- 在本例中，日志显示用户（例如 admin）放弃了在邮件网关的 Web 界面上未提交的所有更改。

```
Thu Oct  8 13:39:44 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /commit, Event: User discarded all uncommitted changes.
```

- 在本例中，日志显示用户（例如 admin）放弃了所有未通过 CLI 提交的更改。

```
Thu Oct  8 13:41:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User discarded all uncommitted changes.
```

- 在本例中，日志显示用户（例如 admin）对 Web UI 会话超时进行了配置更改。

注释 通过查看“配置历史日志”(Configuration History Logs) 或启用审核日志的调试模式，可以查看在邮件网关中进行的配置更改的更多详细信息。

```
Thu Oct  8 13:45:46 2020 Info: Appliance: mail1.example.com, User: admin,
Event: The following configuration changes were commited with comment - 'N/A'
```

```
Thu Oct  8 13:45:46 2020 Info: * [standalone] Number of seconds before the Web UI session
 times out.
```

- 在本例中，日志显示了由于身份验证失败，AsyncOS API 无法获取日志订用。

```
Thu Oct  8 13:52:28 2020 Debug: 08/Oct/2020 13:52:28 +0000 Error - Code: 401,
Details: Unauthorized (No permission -- see authorization schemes)
Thu Oct  8 13:52:28 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,
User: admin, Role: Role Not Available, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Location: GET /esa/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: User is not
valid.
```

- 在本例中，日志显示了由于身份验证成功，AsyncOS API 可以获取日志订用。

```
Thu Oct  8 13:52:37 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,
User: admin, Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,

Location: GET /esa/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: API Access
Success.
```

- 在本例中，日志显示：
  - 使用 CLI 将新用户（例如 admin）添加到了邮件网关，但未提交更改。
  - 使用 CLI 在邮件网关中更新了现有用户账号详细信息，但未提交更改。

```
Thu Oct  8 13:42:48 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin, Source IP: 192.168.1.1, Event: Added user "hops" and changes will reflect
 after commit
Thu Oct  8 13:43:26 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: Updated user "hops" and changes will reflect after commit
```

- 在本例中，日志显示用户（例如 admin）在邮件网关的新 Web 界面上执行了邮件跟踪搜索。

```
Mon Oct 12 04:04:47 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,
User: admin,
Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET /esa/api/v2.0/message-tracking/messages?startDate=2020-10-12T00:00:00.000Z
&endDate=2020-10-12T04:13:00.000Z&ciscoHost=All_Hosts&searchOption=messages&offset=0&limit=100
 HTTP/1.0,
Event: API Access Success.
```

注释 在邮件网关的新Web界面上执行的操作（例如，跟踪，报告或隔离搜索）会根据用于这些操作的相应 API 记录为日志。

使用 CSA 日志

思科安全感知云服务信息会被发布到邮件日志。大多数信息处于“信息”或“调试”级别。

思科安全感知日志条目示例：

- 在本例中，日志显示由于令牌无效，从思科安全感知云服务下载重复点击者列表失败。

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of an invalid token.
```

解决方案：确保您从思科安全感知云服务获取有效的身份验证令牌。

- 在本例中，日志显示由于连接错误，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of a connection error.
```

解决方案：验证用于将邮件网关连接到思科安全感知云服务的防火墙配置设置。

- 在本例中，日志显示由于内部服务器错误，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of an internal server error.
```

解决方案：请联系思科支持部门以获取技术帮助。

- 在本例中，日志显示由于 SSL 证书验证失败，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
the SSL certificate verification failed.
```

解决方案：在邮件网关的自定义证书颁发机构列表中添加代理服务器所需的 CA 证书。

- 在本例中，日志显示由于代理身份验证失败，从思科安全感知云服务下载重复点击者列表失败。

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed
because the proxy authentication failed.
```

解决方案：检查代理服务器是否在邮件网关中配置了正确的身份验证凭证。

- 在本例中，日志显示由于未在思科安全感知云服务上启用报告 API，对思科安全感知云服务的请求失败。

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

解决方案：在思科安全感知云服务的“环境 (Environmental) > 设置 (Settings) > 报告 API (Report API)”选项卡中选中“启用报告 API”(Enable Report API) 复选框。

- 在本例中，日志显示思科安全感知功能在特定日期到期。

```
2020-10-15 08:00:11,968 INFO csa The Cisco Security
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

解决方案：请联系思科客户经理以续订许可证。

- 在本例中，日志显示思科安全感知功能的许可证已过期，并且您的电子邮件网关上已禁用该功能。

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Security
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

解决方案：请联系思科客户经理以续订许可证。

- 在本例中，日志显示下载的重复点击者列表为空。

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

解决方案：在思科安全感知云服务中创建模拟网络钓鱼邮件，并将其发送给组织中的收件人。

- 在本例中，日志显示由于已达到最大下载尝试次数，从思科安全感知云服务下载重复点击者列表失败。

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Security Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

解决方案：请联系思科支持，以增加从思科安全感知云服务下载重复点击者列表的尝试次数。

日志订用

配置日志订用

使用“系统管理”(System Administration) 菜单的“日志订用”(Log Subscriptions)（或在 CLI 中使用 **logconfig** 命令）配置日志订用。日志订用创建存储 AsyncOS 活动信息（包括错误）的日志文件。日志订用将检索或传送（推送）到另一台计算机。通常，日志订用具有以下属性：

Table 32: 日志文件属性

属性	说明
日志类型	定义记录的信息类型和日志订用的格式。有关详细信息，请参阅表：日志类型。
日志名称	用于未来参考的日志订用的别名。

属性	说明
日志字段	选择要包含在给定消息的统一事件日志行中的所需日志字段。 **Note** 默认情况下，系统会选择序列号和 MID 日志字段，并且您无法取消选中这些字段。 **Note** 仅当您将日志订用的日志类型配置为“合并事件日志配置”时，此字段才适用。
文件名	作为文件写入磁盘时的实际名称。如使用多个邮件网关，日志文件名应唯一，以便标识生成日志文件的系统。
按文件大小回滚	回滚之前文件可以达到的最大大小。
按时间回滚	设置文件回滚的时间间隔。
速率限制	在指定的时间范围内（以秒为单位），设置日志文件中记录的最大事件数。 默认时间范围值为 10 秒。
日志级别	设置每个日志订用的明细级别。
检索方法	定义从邮件网关获取日志订用的方法。

日志级别

日志级别决定日志中提供的信息量。日志可以是五种级别中的一种。设置的明细级别越高，创建的日志文件越大，对系统性能的影响也越大。除包含较低级别日志中的所有信息之外，较高级别日志中还包含其他信息。随着明细级别的增加，系统的性能会有所下降。

Note 可以为所有邮件日志类型选择日志级别。

Table 33: 日志级别

日志级别	说明
严重	最低的明细设置。仅记录错误。使用此设置不会监视性能和其他重要活动，但日志文件不会在短时间内达到最大大小。此日志级别相当于系统日志级别“警报”。
Warning	所有错误和系统创建的警告。使用此设置将不允许您监控性能和其他重要活动。此日志级别相当于系统日志级别“警告”。
信息	信息设置可以捕获系统每一秒的操作。例如，打开的连接数或传送尝试次数。该信息级别是推荐的日志级别设置。此日志级别相当于系统日志级别“信息”。

日志级别	说明
调试	如要查明错误的原因，请使用调试日志级别。可临时使用该设置，然后返回默认级别。此日志级别相当于系统日志级别“调试”。
跟踪	建议仅将“跟踪”日志级别供开发人员使用。使用此级别会造成严重的系统性能下降，建议不要使用。此日志级别相当于系统日志级别“调试”(Debug)。

在 GUI 中创建日志订用

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **日志订用 (Log Subscriptions)**。

步骤 2 单击**添加日志订用 (Add Log Subscription)**。

步骤 3 选择日志类型，输入日志名称（用于日志目录）以及日志文件的名称。

步骤 4 [仅适用于合并事件日志] 选择要在给定消息的日志行中包含的所需日志字段。

步骤 5 指定 AsyncOS 在执行日志文件回滚前日志文件可达到的最大大小，以及回滚的时间间隔。有关回滚日志文件的详细信息，请参阅滚动更新日志订用, on page 70。

步骤 6 选择日志级别。可用的选项包括重要、警告、信息、调试或跟踪。

步骤 7 配置日志检索方法。

步骤 8 提交并确认更改。

编辑日志订用

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **日志订用 (Log Subscriptions)**。

步骤 2 单击“日志设置”(Log Settings) 列中的日志名称。

步骤 3 更改日志订用。

步骤 4 提交并确认更改。

配置日志记录的全局设置

系统在文本邮件日志和状态日志中定期记录系统测量数据。使用**系统管理 (System Administration)** > **日志订用 (Log Subscriptions)** 页的“全局设置”部分中的**编辑设置 (Edit Settings)** 按钮（或在 CLI 中使用 `logconfig -> setup` 命令）进行配置：

- 系统测量频率。系统记录性能指标的时间间隔，以秒为单位。

- 是否记录邮件 ID 信头。
- 是否记录远程响应状态代码。
- 是否记录原始邮件的主题信头。
- 应为每封邮件记录的信头列表。

所有日志均可以选择包括以下三种数据：

1. 邮件 ID

   如配置此选项，每封邮件都会记录邮件 ID 信头（如果有）。注意，此邮件 ID 可能来自接收的邮件或可能由 AsyncOS 生成。例如：

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
   ```

2. 远程响应

   如配置此选项，每封邮件均会记录远程响应状态代码（如果有）。例如：

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
   ```

   远程响应字符串是在传输 SMTP 对话期间响应 DATA 命令后收到的人类可读的文本。在本例中，在连接主机发出数据命令后的远程响应是“queued as 9C8B425DA7”。

   ```
   [...]

   250 ok hostname

   250 Ok: queued as 9C8B425DA7
   ```

   空格、标点（以及 250 响应中的 OK 字符）是从字符串开头部分截取的。只有空格是从字符串结尾部分截取的。例如，邮件网关对 DATA 命令默认回应字符串 250 Ok: Message MID accepted。因此，如果远程主机是另一台邮件网关，将记录字符串“Message MID accepted”。

3. 源主题信头

   启用此选项后，日志将记录每封邮件的源主题信头。

   ```
   Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'

   Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
   ```

日志记录邮件信头

有时，当邮件通过系统时，有必要记录邮件信头的存在性及其内容。可以在“日志订用”的“全局设置”页面（或在 CLI 中通过 logconfig -> logheaders 子命令）指定要记录的信头。邮件网关会在文

本邮件日志、传送日志和退回日志中记录指定的邮件信头。如果信头存在，则系统会记录信头的名称和值。如果没有信头，则不会在日志中记录任何信息。

Note 在处理要记录的邮件的过程中，系统会评估存在于邮件中的所有信头，不管是否为日志记录指定了信头都是如此。

SMTP 协议的 RFC 位于 http://www.faqs.org/rfcs/rfc2821.html 并定义用户定义的信头。

如果已通过 logheaders 命令配置了要记录的信头，则在传输信息之后将显示信头信息：

Table 34: Log Headers

信头名称	信头的名称
值	已记录信头的内容

例如，指定“date, x-subject”作为要记录的信头会导致邮件日志中显示以下行目：

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

使用 GUI 配置日志记录的全局设置

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **日志订用 (Log Subscriptions)**。

步骤 2 向下滚动至**全局设置 (Global Settings)** 部分。

步骤 3 单击**编辑设置 (Edit Settings)**。

步骤 4 指定系统测量频率、是否在邮件日志中包含邮件ID信头、是否包含远程响应以及是否包含每封邮件的源主题信头等信息。

步骤 5 输入想要在日志中包含的所有其他信头。

步骤 6 提交并确认更改。

滚动更新日志订用

为防止邮件网关上的日志文件过大，当文件达到用户指定的最大大小或经过一定时间间隔后，AsyncOS 将执行“回滚”、对日志文件存档，并创建新文件来存储传入的日志数据。根据日志订用定义的检索方法，较旧的日志文件将存储在邮件网关上，以供检索或发送至外部计算机。有关如何从邮件网关检索日志文件的详细信息，请参阅日志检索方法, on page 8。

AsyncOS 在回滚日志文件时会执行以下操作：

- 使用回滚时间戳和表示日志文件已保存的字母“**s**”扩展名，对当前日志文件重命名。
- 创建新的日志文件，并使用“**current**”扩展名表明文件为当前文件。
- 将刚刚保存的日志文件发送到远程主机（如使用基于推送的检索方法）。
- 从同一订用传送过去不成功的日志文件（如使用基于推送的检索方法）。
- 超出当前保存的文件总数（如使用基于轮询的检索方法）时，删除日志订用中时间最长的文件。

创建或编辑订用时，可使用 GUI 中的**系统管理 (System Administration) > 日志订用 (Log Subscriptions)** 页面，或在 CLI 中使用 logconfig 命令定义日志订用的回滚设置。触发日志文件回滚的两个设置为：

- 最大文件大小。
- 时间间隔。

按文件大小回滚

当日志文件达到最大文件大小时，AsyncOS 执行日志文件回滚，防止文件占用的磁盘空间过多。定义回滚的最大文件大小时，可使用后缀 m 表示兆字节，使用 k 表示千字节。例如，如希望 AsyncOS 在日志文件达到10 兆字节时进行回滚，可输入 10m。

按时间回滚

如希望定期执行回滚，可选择以下时间间隔之一：

- **无**。AsyncOS 仅在日志文件达到最大文件大小时执行回滚。
- **自定义时间间隔**。AsyncOS 将在上次回滚后经过指定的一段时间再执行回滚。创建计划回滚的自定义时间间隔时，可以 d、h 以及 m 为后缀，分别输入天数、时数以及分钟数。
- **每日回滚**。AsyncOS 每天在指定时间执行回滚。如选择每日回滚，请输入希望 AsyncOS 执行回滚的 24 时制时间，即 HH:MM。

  仅 GUI 提供每日回滚选项。如要在 CLI 中使用 logconfig 命令配置每日回滚，请选择“每周回滚”选项，并使用星号 (*) 指定 AsyncOS 应在每一天执行回滚。

- **每周回滚**。AsyncOS 将在每周的某一天或某几天的指定时间执行回滚。例如，您可以将 AsyncOS 设置为在每周三和每周五的午夜执行日志文件回滚。要配置每周回滚，请选择每周执行回滚的日期和 24 小时制时间 (HH:MM)。

  如使用 CLI，可以使用破折号 (-) 指定天数范围、使用星号 (*) 指定每周的每一天，或逗号 (,) 分隔多个日期和时间。

  下表展示如何使用 CLI 在周三和周五的午夜 (00:00) 对日志订用进行文件回滚。

***Table 35: CLI* 中的每周日志回滚设置**

`Do you want to configure time-based log files rollover? [N]> y`
`Configure log rollover settings:`
`1. Custom time interval.`

```
2. Weekly rollover.
```

```
[1]> 2
```

```
1. Monday
```

```
2. Tuesday
```

```
3. Wednesday
```

```
4. Thursday
```

```
5. Friday
```

```
6. Saturday
```

```
7. Sunday
```

```
Choose the day of week to roll over the log files.  Separate multiple days with comma,

or use "*" to specify every day of a week.
Also you can use dash to specify a range like "1-5":
```

```
[]> 3, 5
```

```
Enter the time of day to rollover log files in 24-hour format (HH:MM).
You can specify hour as "*" to match every hour, the same for minutes.
Separate multiple times of day with comma:
```

```
[]> 00:00
```

按需回滚日志订用

要使用 GUI 即时回滚日志订用，请执行以下操作：

Procedure

步骤 1 在“系统管理”(System Administration) >“日志订用”(Log Subscriptions) 页面上，选中要回滚日志右侧的复选框。

步骤 2 或者，您通过选中“全部”(All) 复选框选择所有日志进行回滚。

步骤 3 选中一个或多个要回滚的日志后，**立即回滚 (Rollover Now)** 按钮随即启用。单击**立即回滚 (Rollover Now)** 按钮可回滚所选日志。

在 GUI 上查看最近的日志条目

准备工作

要通过 GUI 查看日志，必须在管理接口上启用 HTTP 或 HTTPS 服务。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **日志订用 (Log Subscriptions)**。

步骤 2 在表的**日志文件 (Log Files)** 列中，选择日志订用。

步骤 3 登录。

步骤 4 选择一个要在浏览器中查看的日志文件或将其保存到磁盘。

在 CLI 中查看最近的日志条目（tail 命令）

AsyncOS 支持 tail 命令，它显示了在邮件网关上配置的日志的最新条目。发出 tail 命令并选择当前配置的日志的编号以查看它。使用 Ctrl-C 退出 tail 命令。

示例

在以下示例中，tail 命令用于查看系统日志。（此日志跟踪 commit 命令中的用户注释以及其他信息。）tail 命令还接受参数形式的日志名称：tail mail_logs。

```
mail3.example.com> tail

Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download

4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download

6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download

8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download

9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download
```

```
13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download

14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual Download

17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download

19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download

20. "status" Type: "Status Logs" Retrieval: Manual Download

21. "system_logs" Type: "System Logs" Retrieval: Manual Download

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download

23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download


Enter the number of the log you wish to tail.

[]> 19

Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs
config

Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes: Receiving
suspended.

^Cmail3.example.com>
```

配置主机密钥

使用 `logconfig -> hostkeyconfig` 子命令管理从邮件网关向其他服务器推送日志时与 SSH 搭配使用的主机密钥。SSH 服务器必须具有一对主机密钥：一个私钥和一个公钥。专用主机密钥驻留在 SSH 服务器上，无法被远程计算机读取。公共主机密钥可分配给需要与 SSH 服务器交互的任何客户端计算机。

Note 要管理用户密钥，请参阅管理安全外壳 (SSH) 密钥。

`hostkeyconfig` 子命令会执行以下功能：

Table 36: 管理主机密钥 - 子命令列表

命令	说明
New	添加新密钥。
Edit	修改现有密钥。
Delete	删除现有密钥。
Scan	自动下载主机密钥。
Print	显示密钥。
Host	显示系统主机密钥。此值将存入远程系统的“known_hosts”文件。
Fingerprint	显示系统主机密钥指纹。
User	显示将日志推送到远程计算机的系统账户的公共密钥。此密钥与设置 SCP 推送订用时显示的密钥相同。此值将存入远程系统的“authorized_keys”文件。

在下文示例中，AsyncOS 扫描主机密钥并为主机添加密钥：

```
mail3.example.com> logconfig

Currently configured logs:

[ list of logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]> hostkeyconfig

Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.

- DELETE - Remove a key.

- SCAN - Automatically download a host key.
```

```
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan
Please enter the host or IP address to lookup.
[]> mail3.example.com
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]
SSH1:rsa
mail3.example.com 1024 35
[ key displayed ]

Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
2. mail3.example.com ssh-rsa [ key displayed ]
3. mail3.example.com 1024 35 [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
```

```
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
Currently configured logs:
[ list of configured logs ]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
```